

4

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-163661

(43)Date of publication of application : 06.06.2003

(51)Int.Cl. H04L 9/10  
G09C 1/00  
H04L 9/32

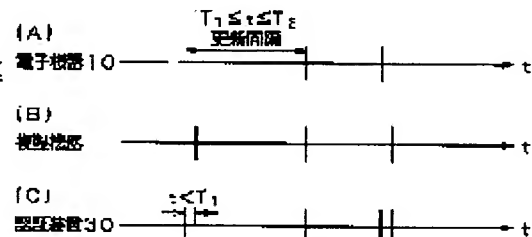
(21)Application number : 2001-361032 (71)Applicant : SONY CORP  
(22)Date of filing : 27.11.2001 (72)Inventor : SAITO SHINYA

#### (54) ELECTRONIC EQUIPMENT, AUTHENTICATION DEVICE, AND SYSTEM AND METHOD FOR DETECTING DUPLICATION EQUIPMENT

##### (57)Abstract:

PROBLEM TO BE SOLVED: To detect the existence of duplication equipment by tracing the duplication equipment.

SOLUTION: In a data transmission and reception system, even when proper electronic equipment 10 informs an authentication device 30 of a request for update always at prescribed intervals with a range  $T_1 \leq t \leq T_2$  as shown in (A), and the duplication equipment informs the authentication device 30 of the request for update at the same intervals as the update intervals of the electronic equipment 10 as shown in (B), a difference is produced between a time when the information of the request reaches the authentication device 30 from the electronic equipment 10 and is accepted and a time when the information of the request reaches the authentication device 30 from the duplication equipment and is accepted. Then, intervals of reaching of the information of the request to the authentication device 30 is deviated from the prescribed range  $T_1 \leq t \leq T_2$  as shown in (C). By taking notice of the deviation and inspecting the compatibility of the updating intervals of key data, the connected duplicating equipment is traced to detect the existence of the duplicated equipment.



データ受信システムにおける更新要求のタイミングの説明図

#### LEGAL STATUS

[Date of request for examination] 29.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-163661

(P2003-163661A)

(43) 公開日 平成15年6月6日 (2003.6.6)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームコード <sup>*</sup> (参考)
H 0 4 L 9/10		G 0 9 C 1/00	6 4 0 E 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 2 1 A
H 0 4 L 9/32			6 7 5 D
			6 7 5 B

審査請求 未請求 請求項の数32 O L (全 27 頁)

(21) 出願番号 特願2001-361032(P2001-361032)

(22) 出願日 平成13年11月27日 (2001. 11. 27)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川 6 丁目 7 番 35 号

(72) 発明者 齊藤 真也

東京都品川区北品川 6 丁目 7 番 35 号 ソニー株式会社内

(74) 代理人 100110434

弁理士 佐藤 勝

F ターム (参考) 5J104 AA07 AA44 EA19 JA21 KA02 KA05

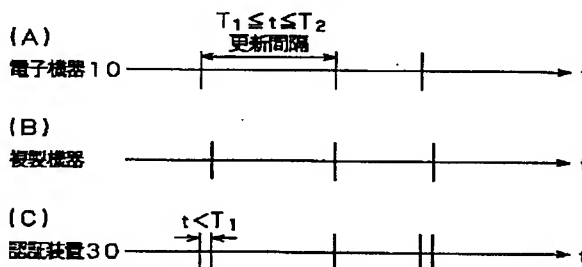
(54) 【発明の名称】 電子機器及び認証装置、並びに複製機器検出システム及び複製機器検出方法

(57) 【要約】

【課題】 複製機器を追跡し、複製機器の存在を検出する。

【解決手段】 データ送受信システムにおいては、

(A) に示すように、正当な電子機器 10 が常に所定の範囲  $T_1 \leq t \leq T_2$  の間隔で、更新のリクエストを認証装置 30 に対して通知し、(B) に示すように、複製機器が電子機器 10 の更新間隔と同間隔で、更新のリクエストを認証装置 30 に対して通知する場合であっても、電子機器 10 から認証装置 30 に対してリクエストの通知が到達して受諾される時刻と、複製機器から認証装置 30 に対してリクエストの通知が到達して受諾される時刻との間に差が生じ、認証装置 30 に対してリクエストの通知が到達する間隔が、(C) に示すように、所定の範囲  $T_1 \leq t \leq T_2$  から外れることに着目し、鍵データの更新間隔の整合性の検証を行うことにより、接続された複製機器を追跡し、複製機器の存在を検出する。



データ送受信システムにおける更新間隔のタイミングの説明図

**【特許請求の範囲】**

【請求項1】 正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を上記認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、上記取得手段によって取得した上記更新時刻情報と、上記乱数発生手段によって前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えることを特徴とする電子機器。

【請求項2】 上記乱数発生手段によって発生した上記乱数値を、次回の公開鍵データの更新までの時間として記憶する記憶手段を備えることを特徴とする請求項1記載の電子機器。

【請求項3】 公開鍵暗号方式における復号を行う復号手段を備え、上記取得手段は、上記認証装置によって上記更新時刻情報が暗号化された暗号化更新時刻情報を取得し、上記復号手段は、上記暗号化更新時刻情報を復号し、上記更新時刻情報を得ることを特徴とする請求項1記載の電子機器。

【請求項4】 上記暗号化更新時刻情報に対する上記認証装置の電子署名の検証を行い、上記暗号化更新時刻情報の検証を行う更新時刻情報検証手段を備えることを特徴とする請求項3記載の電子機器。

【請求項5】 上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が不当なものであると判定された場合に、警告としての暗号化更新時刻情報エラーを示す制御信号を上記認証装置に対して送信する送信手段を備えることを特徴とする請求項4記載の電子機器。

【請求項6】 上記更新間隔検証手段は、上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が正当なものであると判定された場合に、上記公開鍵データの更新間隔の整合性の検証を行うことを特徴とする請求項4記載の電子機器。

【請求項7】 上記更新間隔検証手段による検証の結果、上記複製機器が存在していないものと判定された場合には、上記公開鍵データの更新処理を行うことを特徴とする請求項1記載の電子機器。

【請求項8】 上記更新間隔検証手段による検証の結果、上記複製機器が存在しているものと判定された場合には、警告を発することを特徴とする請求項1記載の電

子機器。

【請求項9】 公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置であって、

所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、

上記更新間隔検証手段による検証の結果に応じた検証結果情報を上記電子機器に対して送信する送信手段とを備えることを特徴とする認証装置。

【請求項10】 上記検証結果情報を上記正当な電子機器の公開鍵データを用いて暗号化する暗号化手段を備え、

上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報を上記電子機器に対して送信することを特徴とする請求項9記載の認証装置。

【請求項11】 上記認証機関の秘密鍵データを用いて上記検証結果情報の電子署名を生成する電子署名生成手段を備え、

上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報と上記電子署名とを上記電子機器に対して送信することを特徴とする請求項10記載の認証装置。

【請求項12】 上記送信手段は、上記更新間隔検証手段による検証の結果、上記差分が上記所定の範囲内にならないものと判定された場合には、上記検証結果情報として、上記更新リクエストを拒否する旨を示す警告情報を上記電子機器に対して送信することを特徴とする請求項9記載の認証装置。

【請求項13】 上記送信手段は、上記更新間隔検証手段による検証の結果、上記差分が上記所定の範囲内にあるものと判定された場合には、上記検証結果情報として、上記更新リクエストを受諾する旨を示す受諾情報を上記電子機器に対して送信することを特徴とする請求項9記載の認証装置。

【請求項14】 正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、

上記電子機器は、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置

に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を上記認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、上記取得手段によって取得した上記更新時刻情報と、上記乱数発生手段によって前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えることを特徴とする複製機器検出システム。

【請求項15】 上記電子機器は、上記乱数発生手段によって発生した上記乱数値を、次の公開鍵データの更新までの時間として記憶する記憶手段を備えることを特徴とする請求項14記載の複製機器検出システム。

【請求項16】 上記認証装置は、上記更新時刻情報を上記正当な電子機器の公開鍵データを用いて暗号化する暗号化手段と、上記暗号化手段によって生成された暗号化更新時刻情報を上記電子機器に対して送信する送信手段とを備えることを特徴とする請求項14記載の複製機器検出システム。

【請求項17】 上記電子機器は、公開鍵暗号方式における復号を行う復号手段を備え、上記取得手段は、上記認証装置における上記暗号化手段によって生成された上記暗号化更新時刻情報を取得し、上記復号手段は、上記暗号化更新時刻情報を復号し、上記更新時刻情報を得ることを特徴とする請求項16記載の複製機器検出システム。

【請求項18】 上記認証装置は、上記認証機関の秘密鍵データを用いて上記暗号化更新時刻情報の電子署名を生成する電子署名生成手段を備え、上記送信手段は、上記暗号化更新時刻情報と上記電子署名とを上記電子機器に対して送信することを特徴とする請求項17記載の複製機器検出システム。

【請求項19】 上記電子機器は、上記暗号化更新時刻情報に対する上記電子署名の検証を行い、上記暗号化更新時刻情報の検証を行う更新時刻情報検証手段を備えることを特徴とする請求項18記載の複製機器検出システム。

【請求項20】 上記電子機器は、上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が不当なものであると判定された場合に、警告としての暗号化更新時刻情報エラーを示す制御信号を上記認証装置に対して送信する他の送信手段を備えることを特徴とする請求項19記載の複製機器検出システム。

【請求項21】 上記更新間隔検証手段は、上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が正当なものであると判定された場合に、上記公開鍵データの更新間隔の整合性

の検証を行うことを特徴とする請求項19記載の複製機器検出システム。

【請求項22】 上記電子機器は、上記更新間隔検証手段による検証の結果、上記複製機器が存在していないものと判定された場合には、上記公開鍵データの更新処理を行うことを特徴とする請求項14記載の複製機器検出システム。

【請求項23】 上記電子機器は、上記更新間隔検証手段による検証の結果、上記複製機器が存在しているものと判定された場合には、警告を発することを特徴とする請求項14記載の複製機器検出システム。

【請求項24】 正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する上記電子機器による公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を上記電子機器によって発生する乱数発生工程と、最後に公開鍵データを更新した時刻を示す更新時刻情報を上記電子機器によって上記認証装置から取得する取得工程と、

現在時刻を示す現在時刻情報と、上記取得工程にて取得した上記更新時刻情報と、上記乱数発生工程にて前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記電子機器によって上記公開鍵データの更新間隔の整合性を検証する更新間隔検証工程とを備えることを特徴とする複製機器検出方法。

【請求項25】 正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、

公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置は、

所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、

上記更新間隔検証手段による検証の結果に応じた検証結果情報を上記電子機器に対して送信する送信手段とを備えることを特徴とする複製機器検出システム。

【請求項 26】 上記認証装置は、上記検証結果情報を上記正当な電子機器の公開鍵データを用いて暗号化する暗号化手段を備え、

上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報を上記電子機器に対して送信することを特徴とする請求項 25 記載の複製機器検出システム。

【請求項 27】 上記電子機器は、上記暗号化手段によって暗号化された上記検証結果情報を上記認証装置から取得する取得手段と、公開鍵暗号方式における復号を行う復号手段とを備え、上記復号手段は、上記取得手段によって取得した暗号化された上記検証結果情報を復号し、上記検証結果情報を得ることを特徴とする請求項 26 記載の複製機器検出システム。

【請求項 28】 上記認証装置は、上記認証機関の秘密鍵データを用いて上記検証結果情報の電子署名を生成する電子署名生成手段を備え、上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報と上記電子署名とを上記電子機器に対して送信することを特徴とする請求項 27 記載の複製機器検出システム。

【請求項 29】 上記電子機器は、上記検証結果情報に対する上記電子署名の検証を行い、上記検証結果情報の検証を行う検証結果情報検証手段を備えることを特徴とする請求項 28 記載の複製機器検出システム。

【請求項 30】 上記送信手段は、上記更新間隔検証手段による検証の結果、上記差分が上記所定の範囲内になりものと判定された場合には、上記検証結果情報として、上記更新リクエストを拒否する旨を示す警告情報を上記電子機器に対して送信することを特徴とする請求項 25 記載の複製機器検出システム。

【請求項 31】 上記送信手段は、上記更新間隔検証手段による検証の結果、上記差分が上記所定の範囲内にあるものと判定された場合には、上記検証結果情報として、上記更新リクエストを受諾する旨を示す受諾情報を上記電子機器に対して送信することを特徴とする請求項 25 記載の複製機器検出システム。

【請求項 32】 正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更

新間隔として予め規定された所定の範囲内にあるか否かを上記認証装置によって検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証工程と、上記更新間隔検証工程による検証の結果に応じた検証結果情報を上記認証装置から上記電子機器に対して送信する送信工程とを備えることを特徴とする複製機器検出方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器及び認証装置、並びに複製機器検出システム及び複製機器検出方法に関する。

【0002】

【従来の技術】 近年、ネットワーク技術の進歩に伴い、いわゆるインターネット等を利用した電子商取引やオンラインショッピング等の各種サービスが普及しつつある。また、ネットワークに接続可能な機器としては、パーソナルコンピュータのような情報処理装置のみならず、例えばデジタルテレビやデジタル衛星放送向けのセットトップボックス等の各種 AV (Audio/Visual) 機器も、ネットワークを介して相互に接続することが可能となりつつある。

【0003】 このようなネットワークシステムにおいては、機器間の通信を行うにあたって、データの盗聴や改竄等の行為による危険を防止するために、通信相手の正当性を認証するための相互認証を行う必要がある。このような機器間認証としては、通常、機器が正当であるか否かを検証するものではなく、当該機器自体は正当であることを前提とした上で、当該機器が所定のサービスを受ける権利を有するものであるか否かを検証するものが多い。

【0004】 具体的には、機器間認証としては、いわゆる共通鍵暗号方式に基づいたチャレンジ／レスポンス型認証が多く用いられる。このチャレンジ／レスポンス型認証とは、認証を受ける機器が固有の秘密情報を有していることを確認することにより、当該機器を認証する方式であり、機器を操作するユーザが所定のチャレンジコードに対するレスポンスコードを入力することにより、正当な機器であることを認証するものである。

【0005】 すなわち、共通鍵暗号方式に基づいた認証を行うネットワークシステムにおいては、機器の認証を行う際には、まず、認証を行う所定の認証装置が、機器に対して所定のチャレンジコードに対するレスポンスコードを返すようにリクエストを行う。そして、ネットワークシステムにおいては、このリクエストに応じて機器が認証装置に対してレスポンスを行うと、認証装置がレスポンスの内容を検証し、当該機器の正当性を判別す

る。

【0006】このように、ネットワークシステムにおいては、共通鍵暗号方式に基づいたチャレンジ/レスポンス型認証を用いることにより、機器間認証を行うことができる。

【0007】

【発明が解決しようとする課題】ところで、上述した共通鍵暗号方式に基づいた認証を行うネットワークシステムにおいては、正当な機器が固有に有する各種情報の一部を複製することによって作製された電子機器である不完全な複製機器が接続された場合には、通常の機器間認証を行うことによって不当なものであることを検証することが可能である。しかしながら、ネットワークシステムにおいては、正当な機器が固有に有する各種情報の全てを複製することによって作製された電子機器である完全な複製機器が接続された場合には、正当な機器であるものと誤って認証されてしまうといった問題があった。

【0008】本発明は、このような実情に鑑みてなされたものであり、不完全な複製機器のみならず、完全な複製機器であっても追跡 (Traitor Tracing) し、複製機器の存在を検出することができる電子機器及び認証装置、並びに複製機器検出システム及び複製機器検出方法を提供することを目的とする。

【0009】

【課題を解決するための手段】上述した目的を達成する本発明にかかる電子機器は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えることを特徴としている。

【0010】このような本発明にかかる電子機器は、現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、更新間隔検証手段によって公開鍵データの更新間隔の整合性を検証する。

【0011】また、上述した目的を達成する本発明にかかる認証装置は、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置であって、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固

有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、この更新間隔検証手段による検証の結果に応じた検証結果情報を電子機器に対して送信する送信手段とを備えることを特徴としている。

【0012】このような本発明にかかる認証装置は、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを更新間隔検証手段によって検証し、公開鍵データの更新間隔の整合性を検証する。

【0013】さらに、上述した目的を達成する本発明にかかる複製機器検出システムは、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、電子機器は、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えることを特徴としている。

【0014】このような本発明にかかる複製機器検出システムは、現在時刻情報と、電子機器によって取得した更新時刻情報と、電子機器によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証する。

【0015】さらにまた、上述した目的を達成する本発明にかかる複製機器検出方法は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する電子機器による公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を電子機器によって発生する乱数発生工程と、最後に公開鍵データを更新した時刻を示す更新時刻情報を電子機器によって認証装置から取得する取得工程と、現在時刻を示す現在時刻情報と、取得工程にて取得した更新時刻情報と、乱数発生工程にて前回の公開鍵データの更新時に発



生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証する更新間隔検証工程とを備えることを特徴としている。

【0016】このような本発明にかかる複製機器検出方法は、現在時刻情報と、電子機器によって取得した更新時刻情報と、電子機器によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証する。

【0017】また、上述した目的を達成する本発明にかかる複製機器検出システムは、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置は、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、この更新間隔検証手段による検証の結果に応じた検証結果情報を電子機器に対して送信する送信手段とを備えることを特徴としている。

【0018】このような本発明にかかる複製機器検出システムは、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証する。

【0019】さらに、上述した目的を達成する本発明にかかる複製機器検出方法は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証工程と、この更新間隔検証工程による検証の結果に応じた検証結果情報を認証装置から電子機器に対して送信する送信工程とを備え

ることを特徴としている。

【0020】このような本発明にかかる複製機器検出方法は、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証する。

【0021】

【発明の実施の形態】以下、本発明を適用した具体的な実施の形態について図面を参照しながら詳細に説明する。

【0022】この実施の形態は、例えば図1に示すように、LAN (Local Area Network) 等の所定のネットワークを介して相互に接続された複数の電子機器10、20の間でデータの送受信を行うことができるデータ送受信システムである。特に、このデータ送受信システムは、正当な電子機器が固有に有する各種情報の一部を複製することによって作製された電子機器である不完全な複製機器が接続された場合のみならず、正当な機器が固有に有する各種情報の全てを複製することによって作製された電子機器である完全な複製機器が接続された場合であっても、複製機器を追跡 (Traitor Tracing) し、複製機器の存在を検出することができるものである。

【0023】このデータ送受信システムは、従来の共通鍵暗号方式に基づく機器間認証 (authentication) を行うものではなく、鍵の配送に関する安全面が向上するとともに鍵の管理が容易であるいわゆる公開鍵暗号方式に基づく機器間認証を行うものである。そこで、ここでは、複製機器の追跡機能についての説明に先だって、公開鍵暗号方式に基づく公開鍵データの登録 (registration)、機器間認証、及び登録又は更新 (renewal) された公開鍵データの更新について説明するものとする。

【0024】データ送受信システムは、例えば図1に示すように、相互に接続された電子機器10、20と、これらの電子機器10、20の認証を行う公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関 (Certification Authority) CAが有する認証装置30とがインターネットNETを介して接続されて構成される。なお、データ送受信システムにおいては、認証機関CAは、1つではなく、電子機器10、20のそれぞれに対応して2つ設けてもよい。

【0025】電子機器10、20は、それぞれ、例えば、パーソナルコンピュータのような情報処理装置の他、デジタルテレビやデジタル衛星放送向けのセットトップボックス等の各種AV (Audio/Visual) 機器として構成され、耐タンパー処理がなされて構成される。電子機器10、20は、それぞれ、図2に示すように、各部を統括的に制御するCPU (Central Processing Unit) 11と、このCPU11のワークエリアとして機能するRAM (Random Access Memory) 12と、CPU11によって実行される各種プログラムを含む情報を格納する読み取り専用のROM (Read Only Memory) 13



と、各種データを記憶する電氣的に書き換え可能なROMであるEEPROM (Electrically Erasable Programmable Read-Only Memory) 14との他に、乱数データを発生する乱数発生部15と、この乱数発生部15によって発生した乱数データを用いて公開鍵暗号方式に用いられる所定の鍵データを生成する鍵生成部16と、公開鍵暗号方式における暗号化及び復号を行う暗号化／復号部17と、外部とデータの送受信を行う通信部18とを備える。電子機器10、20は、それぞれ、これらのCPU11、RAM12、ROM13、EEPROM14、乱数発生部15、鍵生成部16、暗号化／復号部17、及び通信部18がバス19を介して接続されて構成される。

【0026】なお、この電子機器10、20は、それぞれ、乱数発生部15による乱数発生処理、並びに鍵生成部16及び暗号化／復号部17による公開鍵暗号方式に関連する機能を実現する暗号エンジンとしての処理を行うが、この機能をハードウェアで実現するのみならず、コンピュータ実行可能なソフトウェアで実現することもできる。電子機器10、20は、それぞれ、ソフトウェアで実現する場合には、CPU11によって乱数発生処理及び暗号エンジンとしての処理を提供するための所定のプログラムを実行することにより、この機能を実現することができる。このプログラムは、例えばいわゆるコンパクトディスク (Compact Disc: CD) 等のコンピュータ実行可能な所定の記録媒体やインターネット等の伝送媒体によって提供することができる。

【0027】CPU11は、更新間隔検証手段、更新時刻情報検証手段、及び検証結果情報検証手段として機能するものであり、バス19を介して、RAM12、ROM13、EEPROM14、乱数発生部15、鍵生成部16、暗号化／復号部17、及び通信部18と接続し、各部を統括的に制御する。また、CPU11は、図示しないタイマーを有し、このタイマーによって後述するタイマー値を計数したり、現在時刻を提示する。

【0028】RAM12は、CPU11が各種プログラムを実行する際のワークエリアとして機能し、CPU11の制御のもとに、各種データを一時記憶する。

【0029】ROM13は、各種プログラムや、必要に応じて当該電子機器10、20がそれぞれ固有に有する情報である機器固有情報を含む各種データ等の各種情報を格納している。このROM13に格納されている各種プログラムは、CPU11の制御のもとに読み出されて実行されるとともに、このROM13に格納されている各種データは、CPU11の制御のもとに読み出される。

【0030】記憶手段であるEEPROM14は、電氣的に消去、すなわち、書き換え可能なROMであり、CPU11の制御のもとに、上述した機器固有情報や認証機関CAによって発行された公開鍵証明書を含む各種デ

ータを記憶する。また、このEEPROM14に記憶されている各種データは、CPU11の制御のもとに読み出される。

【0031】乱数発生部15は、通信相手の正当性を認証するための相互認証や、この認証後に行うデータ通信の安全性を確保するための暗号化通信に使用する鍵生成の過程等において用いられる乱数データを発生する。この乱数発生部15によって発生された乱数データは、鍵生成部16によって用いられる。また、乱数発生部15は、後述するように、乱数発生手段として、所定の乱数値を発生する。

【0032】鍵生成部16は、所定の公開鍵暗号方式における鍵生成アルゴリズムに基づいて、乱数発生部15によって発生された乱数データを用いて、公開鍵暗号方式における秘密鍵データ及び公開鍵データを生成する。この鍵生成部16によって生成された秘密鍵データ及び公開鍵データは、暗号化／復号部17によって用いられる。

【0033】暗号化／復号部17は、鍵生成部16によって生成された公開鍵データを用いて、所定の公開鍵暗号方式における暗号化を施す。また、暗号化／復号部17は、復号手段として、鍵生成部16によって生成された秘密鍵データを用いて、所定の公開鍵暗号方式における暗号化が施されたデータを復号する。

【0034】通信部18は、送信手段及び取得手段として機能するものであり、暗号化／復号部17によって暗号化が施されたデータや所定の制御信号を外部へと送信するとともに、外部から暗号化が施されたデータを受信する。

【0035】このような電子機器10、20は、それぞれ、後述する所定の通信プロトコルにしたがって、相互に機器間認証を行いつつ、データの送受信を行う。電子機器10、20は、それぞれ、外部へとデータを送信する場合には、鍵生成部16によって生成した所定の公開鍵データを用いて、暗号化／復号部17によって暗号化を施す。また、電子機器10、20は、外部からデータを受信した場合には、鍵生成部16によって生成した所定の秘密鍵データを用いて、暗号化／復号部17によって復号を施す。このとき、電子機器10、20は、それぞれ、公開鍵暗号アルゴリズムとしては任意のものを用いることができ、例えばRSA (Rivest-Shamir-Adleman) 暗号方式や楕円曲線暗号方式 (Elliptic Curve Cipher) 等を用いることができる。

【0036】なお、電子機器10、20は、それぞれ、鍵生成部16及び暗号化／復号部17を公開鍵暗号方式に関連する機能を実現する暗号エンジンとして用いるのみならず、これらの処理に加え、共通鍵暗号方式に関連する機能、特に鍵生成機能を実現する暗号エンジンを併有してもよく、さらに、いわゆるSHA1 (Secure Hash Algorithm 1) 処理等のハッシュ関数を実現する機能

を併有してもよい。

【0037】一方、認証装置30は、認証機関CAが有するものであって、電子機器10、20のそれぞれに対して所定の公開鍵証明書を発行し、電子機器10、20のそれぞれの認証を行う。また、認証装置30は、各種情報を記憶する図示しないリポジトリを有し、機器固有情報や公開鍵データの他、後述するように、最後に鍵データを更新した時刻を示す時刻情報や、電子機器10、20によってアクセスされた時刻を示す時刻情報といった各種情報をリポジトリに記憶させる。

【0038】このような電子機器10、20及び認証装置30から構成されるデータ送受信システムにおいては、後述する所定の通信プロトコルにしたがって、電子機器10、20のそれぞれから認証機関CAにおける認証装置30に対して公開鍵データが登録される。そして、データ送受信システムにおいては、後述する所定の通信プロトコルにしたがって、電子機器10、20が相互に機器間認証を行いつつ、データの送受信が行われる。さらに、データ送受信システムにおいては、後述する所定の通信プロトコルにしたがって、電子機器10、20のそれぞれによって認証機関CAに対して登録又は更新された公開鍵データの更新が行われる。データ送受信システムにおいては、後述するように、この認証機関CAに対する公開鍵データの更新時に、複製機器的存在が検出される。

【0039】さて、このようなデータ送受信システムにおいては、電子機器10、20のそれぞれがインターネットNETに接続されると、これらの電子機器10、20のそれぞれから認証機関CAに対して公開鍵データが登録される。なお、ここでは、電子機器10、20は、それぞれ、認証機関CAによって発行された公開鍵証明書をEEPROM14等に記憶しているものとする。また、ここでは、説明の便宜上、電子機器10が公開鍵データを認証機関CAに対して登録するものとして説明する。

【0040】すなわち、データ送受信システムにおいては、図3に電子機器10と認証機関CAにおける認証装置30との間の通信プロトコルを示すように、電子機器10から認証装置30に対しての公開鍵データの登録リクエストの通知、このリクエストを受信した認証装置30から電子機器10に対してのリクエストに対するレスポンスの通知、このレスポンスを受信した電子機器10から認証装置30に対しての登録情報の送信、及び登録情報を受信した認証装置30から電子機器10に対しての公開鍵データの登録完了又は復号エラーの通知が行われることにより、電子機器10から認証機関CAに対して公開鍵データが登録される。

【0041】具体的には、データ送受信システムにおいては、図4に示すように、電子機器10によって公開鍵データの登録のリクエストを行う旨の所定の操作を行う

と、ステップS1において、電子機器10は、認証装置30に対して、CPU11の制御のもとに、公開鍵データの登録のリクエストを行う旨の所定の制御信号を通信部18を介して送信する。

【0042】これに応じて、データ送受信システムにおいては、ステップS2において、認証装置30は、リクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した認証装置30によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップS3において、認証装置30は、電子機器10に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を送信する。

【0043】続いて、データ送受信システムにおいては、ステップS4において、電子機器10は、通信部18を介してレスポンスを受信すると、ステップS5において、CPU11の制御のもとに、認証機関CAによって発行されてEEPROM14等に記憶している公開鍵証明書Cert(CA)から、認証機関CAの公開鍵データPKCAを取り出す。そして、データ送受信システムにおいては、ステップS6において、電子機器10は、この公開鍵データPKCAを用いて、暗号化/復号部17によって上述した機器固有情報IDMを暗号化し、暗号化機器固有情報E(PKCA, IDM)を生成する。データ送受信システムにおいては、ステップS7において、電子機器10は、生成した暗号化機器固有情報E(PKCA, IDM)と、鍵生成部16によって生成した自己の公開鍵データPKMとを、登録情報として、通信部18を介して認証装置30に対して送信する。

【0044】そして、データ送受信システムにおいては、ステップS8において、認証装置30は、登録情報としての暗号化機器固有情報E(PKCA, IDM)及び公開鍵データPKMを受信すると、ステップS9において、認証機関CAの秘密鍵データSKCAを用いて暗号化機器固有情報E(PKCA, IDM)の復号を試みる。

【0045】データ送受信システムにおいては、認証装置30によって正常に復号を行うことができた場合には、認証装置30は、電子機器10が正当なものであると判断し、ステップS10において、機器固有情報IDMに対する公開鍵データとして公開鍵データPKMをリポジトリ(repository)に記憶させて登録するとともに、公開鍵データPKMの登録処理が正常に完了した旨を通知するために、ステップS11において、正常に登録処理が完了した旨の制御信号を電子機器10に対して送信し、ステップS12において、正常終了する。これに応じて、データ送受信システムにおいては、ステップS13において、正常に登録処理が完了した旨の制御信号を電子機器10が通信部18を介して受信すると、ステップS14において、電子機器10は、正常終了す

る。

【0046】一方、データ送受信システムにおいては、認証装置30によって正常に復号を行うことができなかった場合には、ステップS15において、認証装置30は、警告として、復号エラーを示す制御信号を電子機器10に対して送信し、ステップS16において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS17において、復号エラーを示す制御信号を電子機器10が通信部18を介して受信すると、ステップS18において、電子機器10は、エラー終了する。

【0047】データ送受信システムにおいては、電子機器10がインターネットNETに接続されると、このような一連の処理を経ることにより、電子機器10から認証機関CAに対して公開鍵データPKMを登録することができる。データ送受信システムにおいては、電子機器10によって機器固有情報IDMを認証機関CAの公開鍵データPKCAを用いて暗号化することにより、高い安全性のもとに、公開鍵データPKMの登録を行うことができる。勿論、電子機器20についても同様の処理を経ることにより、認証機関CAに対して自己の公開鍵データを登録することができる。

【0048】なお、データ送受信システムにおいては、電子機器10が認証機関CAによって発行された公開鍵証明書をEEPROM14等に記憶していない場合には、電子機器10は、公開鍵データPKMの登録リクエストを行う際に、認証装置30に対して公開鍵証明書Cert(CA)をリクエストし、受信した公開鍵証明書Cert(CA)に対する認証機関CAの電子署名を検証すればよい。また、データ送受信システムにおいては、暗号化機器固有情報E(PKCA, IDM)及び公開鍵データPKMを登録情報とするのではなく、電子機器10は、公開鍵データPKCAを用いて、機器固有情報IDMとともに自己の公開鍵データPKMをも暗号化し、登録情報としてもよい。さらに、データ送受信システムにおいては、電子機器10は、登録情報である暗号化機器固有情報E(PKCA, IDM)及び公開鍵データPKMに対して自己の秘密鍵データSKMを用いて電子署名を生成し、添付するようにしてもよい。

【0049】つぎに、データ送受信システムにおける機器間認証について説明する。データ送受信システムにおいては、上述した公開鍵データPKMの登録が行われると、電子機器10、20の間でのデータの送受信に先だって、機器間認証が行われる。なお、ここでは、電子機器10、20は、それぞれ、認証機関CAによって発行された公開鍵証明書をEEPROM14等に記憶しているものとする。また、ここでは、電子機器10から電子機器20に対して機器間認証のリクエストを行うものとする。さらに、ここでは、説明の便宜上、電子機器10の認証機関を認証機関CA10と称するとともに、この

認証機関CA10が有する認証装置を認証装置3010と称し、さらに、電子機器20の認証機関を認証機関20と称するとともに、この認証機関CA20が有する認証装置を認証装置3020と称するものとして説明する。

【0050】データ送受信システムにおいては、図5に電子機器10、20と認証装置3010、3020との間の通信プロトコルを示すように、4つのパートに大別された処理、すなわち、電子機器10、20の間での第1の処理、電子機器10と認証装置3020の間での第2の処理、電子機器20と認証装置3010の間での第3の処理、及び電子機器10、20の間での第4の処理を行う。

【0051】すなわち、データ送受信システムにおいては、第1の処理として、電子機器10から電子機器20に対しての機器間認証のリクエストの通知、このリクエストを受信した電子機器20から電子機器10に対してのリクエストに対するレスポンスの通知、電子機器10、20の間での少なくとも公開鍵暗号アルゴリズム及びハッシュアルゴリズムからなる取り決め情報の相互送受信、及び電子機器10、20の間での認証情報の相互送受信が行われ、第2の処理として、電子機器10から認証装置3020に対しての公開鍵証明書発行のリクエストの通知、このリクエストを受信した認証装置3020から電子機器10に対してのリクエストに対するレスポンスの通知、このレスポンスを受信した電子機器10から認証装置3020に対しての電子機器20の暗号化機器固有情報の送信、及び暗号化機器固有情報を受信した認証装置3020から電子機器10に対しての電子機器20の公開鍵証明書の送信が行われ、第3の処理として、電子機器20から認証装置3010に対しての公開鍵証明書発行のリクエストの通知、このリクエストを受信した認証装置3010から電子機器20に対してのリクエストに対するレスポンスの通知、このレスポンスを受信した電子機器20から認証装置3010に対しての電子機器10の暗号化機器固有情報の送信、及び暗号化機器固有情報を受信した認証装置3010から電子機器20に対しての電子機器10の公開鍵証明書の送信が行われ、最後に第4の処理として、電子機器10、20の間での暗号化関数データ及び電子署名の相互送受信が行われることにより、電子機器10、20の間での機器間認証が行われる。

【0052】具体的には、データ送受信システムにおいては、まず図6に示す一連の処理を経ることにより、第1の処理を行う。

【0053】すなわち、データ送受信システムにおいては、同図に示すように、電子機器10によって機器間認証のリクエストを行う旨の所定の操作を行うと、ステップS21において、電子機器10は、電子機器20に対して、CPU11の制御のもとに、機器間認証のリクエ

ストを行う旨の所定の制御信号を通信部18を介して送信する。

【0054】これに応じて、データ送受信システムにおいては、ステップS22において、電子機器20は、通信部18を介してリクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した電子機器20によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップS23において、電子機器20は、電子機器10に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を通信部18を介して送信する。

【0055】続いて、データ送受信システムにおいては、ステップS24において、電子機器10は、通信部18を介してレスポンスを受信すると、ステップS25及びステップS26において、電子機器10、20は、それぞれ、CPU11の制御のもとに、機器間認証を行うために必要となる所定の取り決め情報を通信部18を介して相互に送受信するとともに、この取り決め情報の内容の確認を示す所定の制御信号を通信部18を介して相互に送受信する。ここでは、電子機器10、20は、それぞれ、取り決め情報として、自己が用いる公開鍵暗号アルゴリズムとハッシュアルゴリズムとの他、必要に応じて、所定の臨時データ（nonce data）を相互に送受信する。

【0056】そして、データ送受信システムにおいては、ステップS27において、電子機器10は、自己の認証機関CA10によって発行されてEEPROM14等に記憶している公開鍵証明書Cert（CA10）から、認証機関CA10の公開鍵データPKCA10を取り出す。そして、データ送受信システムにおいては、ステップS28において、電子機器10は、この公開鍵データPKCA10を用いて、暗号化／復号部17によって上述した機器固有情報IDM10を暗号化し、暗号化機器固有情報E（PKCA10、IDM10）を生成する。データ送受信システムにおいては、ステップS29において、電子機器10は、生成した暗号化機器固有情報E（PKCA10、IDM10）と、公開鍵証明書Cert（CA10）とを、認証情報として、通信部18を介して電子機器20に対して送信する。

【0057】一方、データ送受信システムにおいては、ステップS30において、電子機器20は、自己の認証機関CA20によって発行されてEEPROM14等に記憶している公開鍵証明書Cert（CA20）から、認証機関CA20の公開鍵データPKCA20を取り出す。そして、データ送受信システムにおいては、ステップS31において、電子機器20は、この公開鍵データPKCA20を用いて、暗号化／復号部17によって上述した機器固有情報IDM20を暗号化し、暗号化機器固有情報E（PKCA20、IDM20）を生成する。データ送受信システムにおいては、ステップS32にお

いて、電子機器20は、生成した暗号化機器固有情報E（PKCA20、IDM20）と、公開鍵証明書Cert（CA20）とを、認証情報として、通信部18を介して電子機器10に対して送信する。

【0058】続いて、データ送受信システムにおいては、ステップS29において、電子機器20から認証情報としての暗号化機器固有情報E（PKCA20、IDM20）及び公開鍵証明書Cert（CA20）を受信した電子機器10は、ステップS33において、CPU11の制御のもとに、公開鍵証明書Cert（CA20）に対する電子署名の検証を行うことによって公開鍵証明書Cert（CA20）の検証を行う。

【0059】データ送受信システムにおいては、電子機器10による公開鍵証明書Cert（CA20）の検証の結果、公開鍵証明書Cert（CA20）が正当なものであると判定された場合には、第2の処理及び第3の処理へと移行する。一方、データ送受信システムにおいては、電子機器10による公開鍵証明書Cert（CA20）の検証の結果、公開鍵証明書Cert（CA20）が不当なものであると判定された場合には、ステップS34において、電子機器10は、警告として、公開鍵証明書エラーを示す制御信号を通信部18を介して電子機器20に対して送信し、ステップS35において、エラー終了する。これに応じて、データ送受信システムにおいては、公開鍵証明書エラーを示す制御信号を電子機器20が通信部18を介して受信すると、ステップS38において、電子機器20は、エラー終了する。

【0060】一方、データ送受信システムにおいては、ステップS32において、電子機器10から認証情報としての暗号化機器固有情報E（PKCA10、IDM10）及び公開鍵証明書Cert（CA10）を受信した電子機器20は、ステップS36において、CPU11の制御のもとに、公開鍵証明書Cert（CA10）に対する電子署名の検証を行うことによって公開鍵証明書Cert（CA10）の検証を行う。

【0061】データ送受信システムにおいては、電子機器20による公開鍵証明書Cert（CA10）の検証の結果、公開鍵証明書Cert（CA10）が正当なものであると判定された場合には、第2の処理及び第3の処理へと移行する。一方、データ送受信システムにおいては、電子機器20による公開鍵証明書Cert（CA10）の検証の結果、公開鍵証明書Cert（CA10）が不当なものであると判定された場合には、ステップS37において、電子機器20は、警告として、公開鍵証明書エラーを示す制御信号を通信部18を介して電子機器10に対して送信し、ステップS38において、エラー終了する。これに応じて、データ送受信システムにおいては、公開鍵証明書エラーを示す制御信号を電子機器10が通信部18を介して受信すると、ステップS35において、電子機器10は、エラー終了する。

【0062】データ送受信システムにおいては、このような第1の処理を経て、公開鍵証明書Cert(CA10)、Cert(CA20)が正当なものであると判定された場合には、第2の処理及び第3の処理へと移行する。

【0063】まず、第2の処理について説明する。データ送受信システムにおいては、図7に示す一連の処理を経ることにより、第2の処理を行う。

【0064】すなわち、データ送受信システムにおいては、同図に示すように、電子機器10によって電子機器20の公開鍵証明書Cert(IDM20)の発行のリクエストを行う旨の所定の操作を行うと、ステップS41において、電子機器10は、認証装置3020に対して、CPU11の制御のもとに、公開鍵証明書Cert(IDM20)の発行のリクエストを行う旨の所定の制御信号を通信部18を介して送信する。

【0065】これに応じて、データ送受信システムにおいては、ステップS42において、認証装置3020は、リクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した認証装置3020によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップS43において、認証装置3020は、電子機器10に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を送信する。

【0066】続いて、データ送受信システムにおいては、ステップS44において、電子機器10は、通信部18を介してレスポンスを受信すると、ステップS45において、上述した第1の処理にて電子機器20から送信されてきた暗号化機器固有情報E(PKCA20, IDM20)を通信部18を介して認証装置3020に対して送信する。

【0067】そして、データ送受信システムにおいては、ステップS46において、認証装置3020は、暗号化機器固有情報E(PKCA20, IDM20)を受信すると、ステップS47において、認証機関CA20の秘密鍵データSKCA20を用いて暗号化機器固有情報E(PKCA20, IDM20)の復号を試みる。

【0068】データ送受信システムにおいては、認証装置3020によって正常に復号を行うことができなかった場合には、ステップS50において、認証装置3020は、警告として、認証情報エラーを示す制御信号を電子機器10に対して送信し、ステップS51において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS52において、認証情報エラーを示す制御信号を電子機器10が通信部18を介して受信すると、ステップS53において、電子機器10は、エラー終了する。

【0069】一方、データ送受信システムにおいては、認証装置3020によって正常に復号を行うことができ

た場合には、認証装置3020は、ステップS48において、リポジトリを参照し、ステップS49において、電子機器20の機器固有情報IDM20がリポジトリに登録されているか否かを照合する。

【0070】ここで、データ送受信システムにおいては、認証装置3020による照合の結果、機器固有情報IDM20がリポジトリに登録されていないものと判定された場合には、ステップS50において、認証装置3020は、警告として、機器固有情報照合エラーを示す制御信号を電子機器10に対して送信し、ステップS51において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS52において、機器固有情報照合エラーを示す制御信号を電子機器10が通信部18を介して受信すると、ステップS53において、電子機器10は、エラー終了する。

【0071】一方、データ送受信システムにおいては、認証装置3020による照合の結果、機器固有情報IDM20がリポジトリに登録されているものと判定された場合には、認証装置3020は、ステップS54において、リポジトリから機器固有情報IDM20を読み出し、ステップS55において、電子機器20の公開鍵証明書Cert(IDM20)を署名して発行し、ステップS56において、この公開鍵証明書Cert(IDM20)を電子機器10に対して送信する。

【0072】データ送受信システムにおいては、ステップS57において、公開鍵証明書Cert(IDM20)を電子機器10が通信部18を介して受信すると、ステップS58において、電子機器10は、CPU11の制御のもとに、公開鍵証明書Cert(IDM20)に対する認証装置3020の電子署名の検証を行うことによって公開鍵証明書Cert(IDM20)の検証を行う。

【0073】データ送受信システムにおいては、電子機器10による公開鍵証明書Cert(IDM20)の検証の結果、公開鍵証明書Cert(IDM20)が正当なものであると判定された場合には、第4の処理へと移行する。一方、データ送受信システムにおいては、電子機器10による公開鍵証明書Cert(IDM20)の検証の結果、公開鍵証明書Cert(IDM20)が不正なものであると判定された場合には、ステップS59において、電子機器10は、警告として、公開鍵証明書エラーを示す制御信号を通信部18を介して認証装置3020に対して送信し、ステップS60において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS61において、公開鍵証明書エラーを示す制御信号を認証装置3020が受信すると、ステップS62において、認証装置3020は、エラー終了する。

【0074】つぎに、第3の処理について説明する。データ送受信システムにおいては、図8に示す一連の処理

を経ることにより、第3の処理を行う。

【0075】すなわち、データ送受信システムにおいては、同図に示すように、電子機器20によって電子機器10の公開鍵証明書Cert (IDM10)の発行のリクエストを行う旨の所定の操作を行うと、ステップS71において、電子機器20は、認証装置3010に対して、CPU11の制御のもとに、公開鍵証明書Cert (IDM10)の発行のリクエストを行う旨の所定の制御信号を通信部18を介して送信する。

【0076】これに応じて、データ送受信システムにおいては、ステップS72において、認証装置3010は、リクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した認証装置3010によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップS73において、認証装置3010は、電子機器20に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を送信する。

【0077】続いて、データ送受信システムにおいては、ステップS74において、電子機器20は、通信部18を介してレスポンスを受信すると、ステップS75において、上述した第1の処理にて電子機器10から送信されてきた暗号化機器固有情報E (PKCA10, IDM10)を通信部18を介して認証装置3010に対して送信する。

【0078】そして、データ送受信システムにおいては、ステップS76において、認証装置3010は、暗号化機器固有情報E (PKCA10, IDM10)を受信すると、ステップS77において、認証機関CA10の秘密鍵データSKCA10を用いて暗号化機器固有情報E (PKCA10, IDM10)の復号を試みる。

【0079】データ送受信システムにおいては、認証装置3010によって正常に復号を行うことができなかった場合には、ステップS80において、認証装置3010は、警告として、認証情報エラーを示す制御信号を電子機器20に対して送信し、ステップS81において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS82において、認証情報エラーを示す制御信号を電子機器20が通信部18を介して受信すると、ステップS83において、電子機器20は、エラー終了する。

【0080】一方、データ送受信システムにおいては、認証装置3010によって正常に復号を行うことができた場合には、認証装置3010は、ステップS78において、リポジトリを参照し、ステップS79において、電子機器10の機器固有情報IDM10がリポジトリに登録されているか否かを照合する。

【0081】ここで、データ送受信システムにおいては、認証装置3010による照合の結果、機器固有情報IDM10がリポジトリに登録されていないものと判定

された場合には、ステップS80において、認証装置3010は、警告として、機器固有情報照合エラーを示す制御信号を電子機器20に対して送信し、ステップS81において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS82において、機器固有情報照合エラーを示す制御信号を電子機器20が通信部18を介して受信すると、ステップS83において、電子機器20は、エラー終了する。

【0082】一方、データ送受信システムにおいては、認証装置3010による照合の結果、機器固有情報IDM10がリポジトリに登録されているものと判定された場合には、認証装置3010は、ステップS84において、リポジトリから機器固有情報IDM10を読み出し、ステップS85において、電子機器10の公開鍵証明書Cert (IDM10)を署名して発行し、ステップS86において、この公開鍵証明書Cert (IDM10)を電子機器20に対して送信する。

【0083】データ送受信システムにおいては、ステップS87において、公開鍵証明書Cert (IDM10)を電子機器20が通信部18を介して受信すると、ステップS88において、電子機器20は、CPU11の制御のもとに、公開鍵証明書Cert (IDM10)に対する認証装置3010の電子署名の検証を行うことによって公開鍵証明書Cert (IDM10)の検証を行う。

【0084】データ送受信システムにおいては、電子機器20による公開鍵証明書Cert (IDM10)の検証の結果、公開鍵証明書Cert (IDM10)が正当なものであると判定された場合には、第4の処理へと移行する。一方、データ送受信システムにおいては、電子機器20による公開鍵証明書Cert (IDM10)の検証の結果、公開鍵証明書Cert (IDM10)が不当なものであると判定された場合には、ステップS89において、電子機器20は、警告として、公開鍵証明書エラーを示す制御信号を通信部18を介して認証装置3010に対して送信し、ステップS90において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS91において、公開鍵証明書エラーを示す制御信号を認証装置3010が受信すると、ステップS92において、認証装置3010は、エラー終了する。

【0085】データ送受信システムにおいては、このような第2の処理及び第3の処理を経て、公開鍵証明書Cert (IDM10)、Cert (IDM20)が正当なものであると判定された場合には、第4の処理へと移行する。

【0086】データ送受信システムにおいては、図9に示す一連の処理を経ることにより、第4の処理を行う。

【0087】すなわち、データ送受信システムにおいては、同図に示すように、ステップS101において、電



子機器10は、乱数発生部15によって所定のランダム関数に基づいて乱数データ $r_{M10}$ を発生する。

【0088】続いて、データ送受信システムにおいては、電子機器10は、EEPROM14等に記憶している自己の機器固有情報 $ID_{M10}$ を取り出し、ステップS102において、CPU11の制御のもとに、乱数データ $r_{M10}$ と機器固有情報 $ID_{M10}$ とに対して所定の関数 $f$ を適用し、関数データ $f(ID_{M10}, r_{M10})$ を算出する。

【0089】続いて、データ送受信システムにおいては、電子機器10は、ステップS103において、CPU11の制御のもとに、上述した第2の処理にて取得した電子機器20の公開鍵証明書 $Cert(ID_{M20})$ から、電子機器20の公開鍵データ $PK_{M20}$ を取り出す。そして、データ送受信システムにおいては、ステップS104において、電子機器10は、この公開鍵データ $PK_{M20}$ を用いて、暗号化／復号部17によって関数データ $f(ID_{M10}, r_{M10})$ を暗号化し、暗号化関数データ $E(PK_{M20}, f(ID_{M10}, r_{M10}))$ を生成し、さらに、ステップS105において、鍵生成部16によって生成した自己の秘密鍵データ $SK_{M10}$ を用いて、暗号化関数データ $E(PK_{M20}, f(ID_{M10}, r_{M10}))$ の電子署名 $Si_{gM10}$ を生成する。データ送受信システムにおいては、ステップS106において、電子機器10は、生成した暗号化関数データ $E(PK_{M20}, f(ID_{M10}, r_{M10}))$ と、この暗号化関数データ $E(PK_{M20}, f(ID_{M10}, r_{M10}))$ に対する電子署名 $Si_{gM10}$ とを、通信部18を介して電子機器20に対して送信する。

【0090】一方、データ送受信システムにおいては、ステップS107において、電子機器20は、乱数発生部15によって所定のランダム関数に基づいて乱数データ $r_{M20}$ を発生する。

【0091】続いて、データ送受信システムにおいては、電子機器20は、EEPROM14等に記憶している自己の機器固有情報 $ID_{M20}$ を取り出し、ステップS108において、CPU11の制御のもとに、乱数データ $r_{M20}$ と機器固有情報 $ID_{M20}$ とに対して所定の関数 $g$ を適用し、関数データ $g(ID_{M20}, r_{M20})$ を算出する。

【0092】続いて、データ送受信システムにおいては、電子機器20は、ステップS109において、CPU11の制御のもとに、上述した第3の処理にて取得した電子機器10の公開鍵証明書 $Cert(ID_{M10})$ から、電子機器10の公開鍵データ $PK_{M10}$ を取り出す。そして、データ送受信システムにおいては、ステップS110において、電子機器20は、この公開鍵データ $PK_{M10}$ を用いて、暗号化／復号部17によって関数データ $g(ID_{M20}, r_{M20})$ を暗号化し、暗号

化関数データ $E(PK_{M10}, g(ID_{M20}, r_{M20}))$ を生成し、さらに、ステップS111において、鍵生成部16によって生成した自己の秘密鍵データ $SK_{M20}$ を用いて、暗号化関数データ $E(PK_{M10}, g(ID_{M20}, r_{M20}))$ の電子署名 $Si_{gM20}$ を生成する。データ送受信システムにおいては、ステップS112において、電子機器20は、生成した暗号化関数データ $E(PK_{M10}, g(ID_{M20}, r_{M20}))$ と、この暗号化関数データ $E(PK_{M10}, g(ID_{M20}, r_{M20}))$ に対する電子署名 $Si_{gM20}$ とを、通信部18を介して電子機器10に対して送信する。

【0093】続いて、データ送受信システムにおいては、ステップS106において、電子機器20から暗号化関数データ $E(PK_{M10}, g(ID_{M20}, r_{M20}))$ 及び電子署名 $Si_{gM20}$ を受信した電子機器10は、ステップS113において、CPU11の制御のもとに、電子機器20の公開鍵証明書 $Cert(ID_{M20})$ から、電子機器20の公開鍵データ $PK_{M20}$ を取り出し、ステップS114において、暗号化関数データ $E(PK_{M10}, g(ID_{M20}, r_{M20}))$ に対する電子署名 $Si_{gM20}$ の検証を行う。

【0094】データ送受信システムにおいては、電子機器10による電子署名 $Si_{gM20}$ の検証の結果、電子署名 $Si_{gM20}$ が不当なものであると判定された場合には、ステップS115において、電子機器10は、警告として、電子署名エラーを示す制御信号を通信部18を介して電子機器20に対して送信し、ステップS116において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS121において、電子署名エラーを示す制御信号を電子機器20が通信部18を介して受信すると、ステップS122において、電子機器20は、エラー終了する。一方、データ送受信システムにおいては、電子署名 $Si_{gM20}$ の検証の結果、電子署名 $Si_{gM20}$ が正当なものであると判定された場合には、ステップS117において、電子機器10は、鍵生成部16によって生成した自己の秘密鍵データ $SK_{M10}$ を用いて、電子機器20から送信されてきた暗号化関数データ $E(PK_{M10}, g(ID_{M20}, r_{M20}))$ の復号を試みる。

【0095】データ送受信システムにおいては、電子機器10によって正常に復号を行うことができなかった場合には、ステップS115において、電子機器10は、警告として、復号エラーを示す制御信号を通信部18を介して電子機器20に対して送信し、ステップS116において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS121において、復号エラーを示す制御信号を電子機器20が通信部18を介して受信すると、ステップS122において、電子機



器20は、エラー終了する。

【0096】一方、データ送受信システムにおいては、電子機器10によって正常に復号を行うことができた場合には、電子機器10は、ステップS118において、関数データ $f$  ( $IDM10$ ,  $rM10$ ) と、復号して得られた関数データ $g$  ( $IDM20$ ,  $rM20$ ) とに対して所定のハッシュ関数 $Hash$ を適用し、 $Hash(f(IDM10, rM10), g(IDM20, rM20))$ を共通鍵データ、すなわち、対称鍵 (symmetric key) データとして生成して正常終了する。

【0097】また、データ送受信システムにおいては、ステップS112において、電子機器10から暗号化関数データ $E(PKM20, f(IDM10, rM10))$ 及び電子署名 $Si gM10$ を受信した電子機器20は、ステップS119において、CPU11の制御のもとに、電子機器10の公開鍵証明書 $Cert(IDM10)$ から、電子機器10の公開鍵データ $PKM10$ を取り出し、ステップS120において、暗号化関数データ $E(PKM20, f(IDM10, rM10))$ に対する電子署名 $Si gM10$ の検証を行う。

【0098】データ送受信システムにおいては、電子機器20による電子署名 $Si gM10$ の検証の結果、電子署名 $Si gM10$ が不当なものであると判定された場合には、ステップS121において、電子機器20は、警告として、電子署名エラーを示す制御信号を通信部18を介して電子機器10に対して送信し、ステップS122において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS115において、電子署名エラーを示す制御信号を電子機器10が通信部18を介して受信すると、ステップS116において、電子機器10は、エラー終了する。一方、データ送受信システムにおいては、電子署名 $Si gM10$ の検証の結果、電子署名 $Si gM10$ が正当なものであると判定された場合には、ステップS123において、電子機器20は、鍵生成部16によって生成した自己の秘密鍵データ $SKM20$ を用いて、電子機器10から送信されてきた暗号化関数データ $E(PKM20, g(IDM10, rM10))$ の復号を試みる。

【0099】データ送受信システムにおいては、電子機器20によって正常に復号を行うことができなかった場合には、ステップS121において、電子機器20は、警告として、復号エラーを示す制御信号を通信部18を介して電子機器10に対して送信し、ステップS122において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS115において、復号エラーを示す制御信号を電子機器10が通信部18を介して受信すると、ステップS116において、電子機器10は、エラー終了する。

【0100】一方、データ送受信システムにおいては、

電子機器20によって正常に復号を行うことができた場合には、電子機器20は、ステップS124において、関数データ $g(IDM20, rM20)$ と、復号して得られた関数データ $f(IDM10, rM10)$ とに対して所定のハッシュ関数 $Hash$ を適用し、 $Hash(f(IDM10, rM10), g(IDM20, rM20))$ を共通鍵データとして生成して正常終了する。

【0101】データ送受信システムにおいては、このような第1の処理乃至第4の処理からなる一連の処理を経ることにより、電子機器10、20の間での機器間認証を行うことができる。これにより、データ送受信システムにおいては、電子機器10、20が不当に機能追加や機能削除が施されて改造された不完全な複製機器ではなく、また、不当に偽造された不完全な複製機器ではないことが認証され、電子機器10、20の間でのデータの送受信が可能とされる。なお、上述した第2の処理及び第3の処理を正常終了した段階で、電子機器10、20は、それぞれ、互いの公開鍵証明書 $Cert(IDM10)$ 、 $Cert(IDM20)$ を取得していることから、データ送受信システムにおいては、第4の処理にて臨時データとして種々のパラメータを与えることにより、第4の処理として、無数のパターンを構築することができる。ここでは、データ送受信システムは、電子機器10、20が、それぞれ、互いの公開鍵証明書 $Cert(IDM10)$ 、 $Cert(IDM20)$ を取得することができること、及び共通鍵データを生成することができることにより、機器間認証を行うことができる。

【0102】なお、データ送受信システムにおいては、上述した乱数データ $rM10$ 、 $rM20$ を発生するのに用いるランダム関数としては、電子機器10、20の間で同一のものであってもよく、異なるものであってもよい。また、データ送受信システムにおいては、上述した関数 $f$ 及び関数 $g$ としては、電子機器10、20の間で同一のものであってもよく、異なるものであってもよい。さらに、データ送受信システムにおいては、電子機器10の認証機関 $CA10$ と電子機器20の認証機関 $CA20$ とは、同一であってもよい。

【0103】また、データ送受信システムにおいては、電子機器10、20が、それぞれ、自己の認証機関 $CA10$ 、 $CA20$ によって発行された公開鍵証明書をEEPROM14等に記憶していない場合には、電子機器10、20は、それぞれ、自己の認証装置3010、3020に対して公開鍵証明書 $Cert(CA10)$ 、 $Cert(CA20)$ をリクエストし、受信した公開鍵証明書 $Cert(CA10)$ 、 $Cert(CA20)$ に対する認証機関 $CA10$ 、 $CA20$ の電子署名を検証すればよい。また、データ送受信システムにおいては、電子機器10、20は、それぞれ、上述した認証情報の相互送受信の際や、認証装置3010、3020に対する暗号

化機器固有情報E (PKCA10, IDM10), E (PKCA20, IDM20) の送信の際に、自己が生成した電子署名を添付するようにしてもよい。

【0104】 つぎに、データ送受信システムにおける登録又は更新された公開鍵データの更新について説明する。データ送受信システムにおいては、所定のタイミングで発せされる電子機器10, 20のそれぞれからのリクエストに応じて、認証機関CAに対して登録又は更新された公開鍵データが更新される。なお、ここでは、電子機器10, 20は、それぞれ、認証機関CAによって発行された公開鍵証明書をEEPROM14等に記憶しているものとする。また、ここでは、説明の便宜上、電子機器10が認証機関CAに対して登録又は更新された公開鍵データを更新するものとして説明する。

【0105】 すなわち、データ送受信システムにおいては、図10に電子機器10と認証機関CAにおける認証装置30との間の通信プロトコルを示すように、電子機器10から認証装置30に対しての公開鍵データの更新リクエストの通知、このリクエストを受信した認証装置30から電子機器10に対してのリクエストに対するレスポンスの通知、このレスポンスを受信した電子機器10から認証装置30に対しての更新情報の送信、及び更新情報を受信した認証装置30から電子機器10に対しての公開鍵データの更新完了又は復号エラー若しくは機器固有情報照合エラーの通知が行われることにより、電子機器10から認証機関CAに対して登録又は更新された公開鍵データが更新される。

【0106】 具体的には、データ送受信システムにおいては、図11に示すように、電子機器10によって公開鍵データの更新のリクエストを行う旨の所定の操作を行うと、ステップS131において、電子機器10は、認証装置30に対して、CPU11の制御のもとに、公開鍵データの更新のリクエストを行う旨の所定の制御信号を通信部18を介して送信する。

【0107】 これに応じて、データ送受信システムにおいては、ステップS132において、認証装置30は、リクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した認証装置30によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップS133において、認証装置30は、電子機器10に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を送信する。

【0108】 続いて、データ送受信システムにおいては、ステップS134において、電子機器10は、通信部18を介してレスポンスを受信すると、ステップS135において、CPU11の制御のもとに、認証機関CAによって発行されてEEPROM14等に記憶している公開鍵証明書Cert (CA) から、認証機関CAの公開鍵データPKCAを取り出す。そして、データ送受信システムにおいては、ステップS136において、電

子機器10は、この公開鍵データPKCAを用いて、暗号化／復号部17によって上述した機器固有情報IDMを暗号化し、暗号化機器固有情報E (PKCA, IDM) を生成する。データ送受信システムにおいては、ステップS137において、電子機器10は、生成した暗号化機器固有情報E (PKCA, IDM) と、鍵生成部16によって生成した自己の新たな公開鍵データPKMnewとを、更新情報として、通信部18を介して認証装置30に対して送信する。

【0109】 そして、データ送受信システムにおいては、ステップS138において、認証装置30は、更新情報としての暗号化機器固有情報E (PKCA, IDM) 及び新たな公開鍵データPKMnewを受信すると、ステップS139において、認証機関CAの秘密鍵データSKCAを用いて暗号化機器固有情報E (PKCA, IDM) の復号を試みる。

【0110】 データ送受信システムにおいては、認証装置30によって正常に復号を行うことができた場合には、認証装置30は、ステップS140において、リポトリを参照し、ステップS141において、復号して得られた機器固有情報IDMがリポトリに登録されているか否かを照合する。

【0111】 ここで、データ送受信システムにおいては、認証装置30による照合の結果、機器固有情報IDMがリポトリに登録されていないものと判定された場合には、ステップS148において、認証装置30は、警告として、機器固有情報照合エラーを示す制御信号を電子機器10に対して送信し、ステップS149において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS150において、機器固有情報照合エラーを示す制御信号を電子機器10が通信部18を介して受信すると、ステップS151において、電子機器10は、エラー終了する。

【0112】 一方、データ送受信システムにおいては、認証装置30による照合の結果、機器固有情報IDMがリポトリに登録されているものと判定された場合には、認証装置30は、電子機器10が前回公開鍵データの登録又は更新を行ったものと同じの正当なものであると判断し、ステップS142及びステップS143において、機器固有情報IDMに対する公開鍵データとして新たな公開鍵データPKMnewをリポトリに記憶させて更新するとともに、公開鍵データPKMnewの更新処理が正常に完了した旨を通知するために、ステップS144において、正常に更新処理が完了した旨の制御信号を電子機器10に対して送信し、ステップS145において、正常終了する。これに応じて、データ送受信システムにおいては、ステップS146において、正常に更新処理が完了した旨の制御信号を電子機器10が通信部18を介して受信すると、ステップS147において、電子機器10は、正常終了する。

【0113】一方、データ送受信システムにおいては、認証装置30によって正常に復号を行うことができなかった場合には、ステップS148において、認証装置30は、警告として、復号エラーを示す制御信号を電子機器10に対して送信し、ステップS149において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップS150において、復号エラーを示す制御信号を電子機器10が通信部18を介して受信すると、ステップS151において、電子機器10は、エラー終了する。

【0114】データ送受信システムにおいては、このような一連の処理を経ることにより、電子機器10が認証機関CAに対して登録又は更新された公開鍵データを新たな公開鍵データ $PK_{Mnew}$ に更新することができる。データ送受信システムにおいては、電子機器10によって機器固有情報 $ID_M$ を認証機関CAの公開鍵データ $PK_{CA}$ を用いて暗号化することにより、高い安全性のもとに、公開鍵データ $PK_{Mnew}$ の更新を行うことができる。勿論、電子機器20についても同様の処理を経ることにより、認証機関CAに対して自己の公開鍵データを登録することができる。

【0115】なお、データ送受信システムにおいては、電子機器10が認証機関CAによって発行された公開鍵証明書をEEPROM14等に記憶していない場合には、電子機器10は、公開鍵データ $PK_{Mnew}$ の更新リクエストを行う際に、認証装置30に対して公開鍵証明書 $Cert(CA)$ をリクエストし、受信した公開鍵証明書 $Cert(CA)$ に対する認証機関CAの電子署名を検証すればよい。また、データ送受信システムにおいては、暗号化機器固有情報 $E(PK_{CA}, ID_M)$ 及び公開鍵データ $PK_{Mnew}$ を更新情報とするのではなく、電子機器10は、公開鍵データ $PK_{CA}$ を用いて、機器固有情報 $ID_M$ とともに自己の公開鍵データ $PK_{Mnew}$ をも暗号化し、更新情報としてもよい。さらに、データ送受信システムにおいては、電子機器10は、更新情報である暗号化機器固有情報 $E(PK_{CA}, ID_M)$ 及び公開鍵データ $PK_{Mnew}$ に対して自己の古い秘密鍵データ $SK_M$ 、又は自己の新たな秘密鍵データ $SK_{Mnew}$ を用いて電子署名を生成し、添付するようにしてもよい。

【0116】さて、データ送受信システムは、正当な電子機器が固有に有する各種情報の一部を複製することによって作製された電子機器である不完全な複製機器が接続された場合のみならず、正当な機器が固有に有する各種情報の全てを複製することによって作製された電子機器である完全な複製機器が接続された場合であっても、認証機関CAに対する公開鍵データの更新時に、複製機器を追跡することができ、複製機器の存在を検出することができる。ここでは、説明の便宜上、正当な機器である電子機器10とこの電子機器10の複製機器とが接続

された場合について説明する。

【0117】概念的には、データ送受信システムにおいては、公開鍵データの更新を行う際には、図12に示すように、電子機器10及び複製機器ともに、同様の動作を行う。すなわち、電子機器10及び複製機器は、それぞれ、乱数値 $t$ を発生し、この発生した乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たすか否かを判定する。そして、電子機器10及び複製機器は、それぞれ、乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たさない場合には、再度異なる乱数値 $t$ を発生し、この乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たすか否かを判定する。一方、電子機器10及び複製機器は、それぞれ、乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たす場合には、新たな公開鍵データ及び秘密鍵データの対を生成し、先に図10に示した更新処理のプロトコルにしたがって、先に図11に示したような処理を行い、認証装置30に対する公開鍵データの更新を行う。

【0118】ここで、データ送受信システムにおいては、機器固有情報 $ID_M$ を有する機器の公開鍵データ及び秘密鍵データの対の更新間隔は、常に、予め規定された所定の範囲 $T_1 \leq t \leq T_2$ である必要があることに着目する。

【0119】すなわち、データ送受信システムにおいては、図13(A)に示すように、正当な機器である電子機器10が常に所定の範囲 $T_1 \leq t \leq T_2$ の間隔で、更新のリクエストを認証装置30に対して通知する場合であり、同図(B)に示すように、複製機器が電子機器10の更新間隔と同間隔で、更新のリクエストを認証装置30に対して通知する場合であっても、電子機器10から認証装置30に対してリクエストの通知が到達して受諾される時刻と、複製機器から認証装置30に対してリクエストの通知が到達して受諾される時刻との間に差が生じることから、複製機器、特に完全な複製機器が存在する場合には、認証装置30に対してリクエストの通知が到達する間隔は、同図(C)に示すように、例えば $t < T_1$ といったように、所定の範囲 $T_1 \leq t \leq T_2$ から外れる。このとき、データ送受信システムにおいては、たとえ、電子機器10から認証装置30に対してリクエストの通知が発せられる時刻と、複製機器から認証装置30に対してリクエストの通知が発せられる時刻とが同一であったとしても、認証装置30によってリクエストを受諾する際には時間的なずれが生じることから、結果的に、認証装置30に対してリクエストの通知が到達する間隔は、規定された所定の範囲 $T_1 \leq t \leq T_2$ から必然的に外れることとなる。

【0120】したがって、データ送受信システムにおいては、この鍵データの更新間隔のずれを検出することにより、複製機器を追跡し、複製機器の存在を検出することができる。

【0121】具体的には、データ送受信システムにおい

ては、図14乃至図16に示す一連の処理を経ることにより、複製機器を追跡し、その存在を検出する。

【0122】まず、鍵データの更新間隔の整合性の検証を電子機器10によって行う場合について、図14を用いて説明する。

【0123】データ送受信システムにおいては、同図に示すように、ステップS161において、電子機器10は、CPU11の制御のもとに、上述したタイマーが計数するタイマー値が“0”であるか否かを判定する。データ送受信システムにおいては、タイマー値が“0”でないものと判定された場合には、ステップS162において、電子機器10は、CPU11の制御のもとに、タイマー値を“1”だけデクリメントさせ、タイマー値が“0”であるか否かを再度判定する。

【0124】そして、データ送受信システムにおいては、電子機器10は、このような処理をタイマー値が“0”となるまで繰り返し、タイマー値が“0”であるものと判定された場合には、ステップS163において、CPU11の制御のもとに、乱数発生部15によって乱数値 $t$ を発生し、ステップS164において、CPU11の制御のもとに、この乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たすか否かを判定する。データ送受信システムにおいては、電子機器10は、乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たさない場合には、ステップS163からの処理を繰り返し、発生した乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たすまで、乱数値 $t$ を発生する。

【0125】データ送受信システムにおいては、電子機器10は、乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たす場合には、ステップS165において、CPU11の制御のもとに、この乱数値 $t$ を次の鍵データの更新までの時間 $timer\_n$ としてEEPROM14等に記憶させる。

【0126】これと同時に、データ送受信システムにおいては、ステップS166において、電子機器10は、認証装置30に対して、CPU11の制御のもとに、最後に鍵データを更新した時刻を示す更新時刻情報 $T_{last}$ のリクエストを行う旨の所定の制御信号を通信部18を介して送信する。なお、ここでの更新時刻情報 $T_{last}$ は、最後に先に図11に示したステップS142及びステップS143にて新たな公開鍵データ $PKM_{new}$ をリポジトリに記憶させて更新した時刻を示すものとする。いずれにせよ、認証装置30は、この更新時刻情報 $T_{last}$ をリポジトリ等に記憶している必要がある。

【0127】これに応じて、データ送受信システムにおいては、ステップS167において、認証装置30は、リクエストを受信すると、電子機器10の公開鍵データ $PKM$ を用いてリクエストされた更新時刻情報 $T_{last}$ を暗号化し、暗号化更新時刻情報 $E(PKM, T_{last})$ を生成するとともに、認証機関CAの秘密

鍵データ $SK_{CA}$ を用いて暗号化更新時刻情報 $E(PKM, T_{last})$ の電子署名 $Sig$ を生成し、ステップS168において、レスポンスとして、生成した暗号化更新時刻情報 $E(PKM, T_{last})$ と、この暗号化更新時刻情報 $E(PKM, T_{last})$ に対する電子署名 $Sig$ とを、電子機器10に対して送信する。

【0128】続いて、データ送受信システムにおいては、ステップS169において、電子機器10は、認証装置30から暗号化更新時刻情報 $E(PKM, T_{last})$ 及び電子署名 $Sig$ を受信すると、ステップS170において、CPU11の制御のもとに、電子署名 $Sig$ の検証を行うことによって暗号化更新時刻情報 $E(PKM, T_{last})$ の検証を行う。

【0129】データ送受信システムにおいては、電子機器10による暗号化更新時刻情報 $E(PKM, T_{last})$ の検証の結果、暗号化更新時刻情報 $E(PKM, T_{last})$ が不当なものであると判定された場合には、ステップS173において、電子機器10は、警告として、暗号化更新時刻情報エラーを示す制御信号を通信部18を介して認証装置30に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化更新時刻情報エラーを示す制御信号を認証装置30が受信すると、認証装置30は、エラー終了する。

【0130】一方、データ送受信システムにおいては、電子機器10による暗号化更新時刻情報 $E(PKM, T_{last})$ の検証の結果、暗号化更新時刻情報 $E(PKM, T_{last})$ が正当なものであると判定された場合には、ステップS171において、電子機器10は、CPU11の制御のもとに、現在時刻を示す現在時刻情報 $T_{now}$ と、暗号化／復号部17によって暗号化更新時刻情報 $E(PKM, T_{last})$ を復号して得られた更新時刻情報 $T_{last}$ と、前回のタイマー値、すなわち、前回の鍵データの更新時にステップS165においてEEPROM14等に記憶させた時間 $timer\_n$ に相当するタイマー値 $timer$ とに基づいて、

$T_{now} - (T_{last} + timer) \leq \varepsilon$

を満たすか否かを判定する。ここで、定数 $\varepsilon$ は、電子機器10と認証装置30との間でのパケットの受け渡しに要する時間や、電子機器10の内部での処理時間等を吸収する固定値である。また、現在時刻情報 $T_{now}$ は、このステップS171における時刻を示すものとする。

【0131】データ送受信システムにおいては、 $T_{now} - (T_{last} + timer) \leq \varepsilon$ を満たすものと判定された場合には、複製機器が存在していないことを示すことから、ステップS172において、電子機器10は、鍵データの更新処理へと移行し、先に図10に示した更新処理のプロトコルにしたがって、先に図11に示したような処理を行い、認証装置30に対する公開鍵データの更新を行う。

【0132】一方、データ送受信システムにおいては、 $T_{now} - (T_{last} + timer) \leq \varepsilon$ を満たさないものと判定された場合には、複製機器が存在していることを示すことから、ステップS173において、電子機器10は、警告を発し、認証装置30に対してその旨を通知するとともに、複製機器に対抗するための所定の処理へと移行する。電子機器10は、複製機器に対抗するための所定の処理として、例えば、自己が提供するサービスを停止する処理や、自己の電源を遮断する処理といった種々の処理を行うことができる。

【0133】このように、データ送受信システムは、鍵データの更新間隔の整合性の検証を電子機器10の側で行うことにより、複製機器を追跡してその存在を検出することができる。

【0134】つぎに、鍵データの更新間隔の整合性の検証を認証装置30によって行う場合について、図15を用いて説明する。

【0135】データ送受信システムにおいては、同図に示すように、ステップS181において、電子機器10は、CPU11の制御のもとに、上述したタイマーが計数するタイマー値が“0”であるか否かを判定する。データ送受信システムにおいては、タイマー値が“0”でないものと判定された場合には、ステップS182において、電子機器10は、CPU11の制御のもとに、タイマー値を“1”だけデクリメントさせ、タイマー値が“0”であるか否かを再度判定する。

【0136】そして、データ送受信システムにおいては、電子機器10は、このような処理をタイマー値が“0”となるまで繰り返し、タイマー値が“0”であるものと判定された場合には、ステップS183において、CPU11の制御のもとに、乱数発生部15によって乱数値 $t$ を発生し、ステップS184において、CPU11の制御のもとに、この乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たすか否かを判定する。データ送受信システムにおいては、電子機器10は、乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たさない場合には、ステップS183からの処理を繰り返し、発生した乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たすまで、乱数値 $t$ を発生する。

【0137】データ送受信システムにおいては、電子機器10は、乱数値 $t$ が所定の範囲 $T_1 \leq t \leq T_2$ を満たす場合には、ステップS185において、CPU11の制御のもとに、この乱数値 $t$ を次の鍵データの更新までの時間 $timer\_n$ としてEEPROM14等に記憶させる。

【0138】これと同時に、データ送受信システムにおいては、ステップS186において、電子機器10は、認証装置30に対して、CPU11の制御のもとに、鍵データの更新のリクエストを行う旨の所定の制御信号を通信部18を介して送信する。

【0139】これに応じて、データ送受信システムにお

いては、ステップS187において、認証装置30は、リクエストを受信すると、ステップS188において、最後に鍵データを更新した時刻を示す更新時刻情報 $T_{last}$ と、電子機器10によってアクセスされた時刻を示すアクセス時刻情報 $T_{acs}$ とを用いて、

$T_1 \leq (T_{acs} - T_{last}) + \varepsilon \leq T_2$ を満たすか否かを判定する。ここで、定数 $\varepsilon$ は、上述したように、電子機器10と認証装置30との間でのパケットの受け渡しに要する時間や、電子機器10の内部での処理時間等を吸収する固定値である。また、ここでの更新時刻情報 $T_{last}$ は、最後に先に図11に示したステップS142及びステップS143にて新たな公開鍵データ $PK_{M_{new}}$ をリポジトリに記憶させて更新した時刻を示すものとする。いずれにせよ、認証装置30は、この更新時刻情報 $T_{last}$ をリポジトリ等に記憶している必要がある。さらに、アクセス時刻情報 $T_{acs}$ は、このステップS188における時刻を示すものとする。

【0140】データ送受信システムにおいては、 $T_1 \leq (T_{acs} - T_{last}) + \varepsilon \leq T_2$ を満たさないものと判定された場合には、認証装置30は、電子機器10の公開鍵データ $PK_M$ を用いて、鍵データの更新のリクエストを拒否する旨を示す検証結果情報としての警告情報 $MSG_{alert}$ を暗号化し、暗号化警告情報 $E(PK_M, MSG_{alert})$ を生成するとともに、認証機関CAの秘密鍵データ $SK_{CA}$ を用いて暗号化警告情報 $E(PK_M, MSG_{alert})$ の電子署名 $Sig$ を生成し、ステップS189において、レスポンスとして、生成した暗号化警告情報 $E(PK_M, MSG_{alert})$ と、この暗号化警告情報 $E(PK_M, MSG_{alert})$ に対する電子署名 $Sig$ とを、電子機器10に対して送信する。

【0141】一方、データ送受信システムにおいては、 $T_1 \leq (T_{acs} - T_{last}) + \varepsilon \leq T_2$ を満たすものと判定された場合には、認証装置30は、電子機器10の公開鍵データ $PK_M$ を用いて、鍵データの更新のリクエストを受諾する旨を示す検証結果情報としての受諾情報 $MSG_{OK}$ を暗号化し、暗号化受諾情報 $E(PK_M, MSG_{OK})$ を生成するとともに、認証機関CAの秘密鍵データ $SK_{CA}$ を用いて暗号化受諾情報 $E(PK_M, MSG_{OK})$ の電子署名 $Sig$ を生成し、ステップS190において、レスポンスとして、生成した暗号化受諾情報 $E(PK_M, MSG_{OK})$ と、この暗号化受諾情報 $E(PK_M, MSG_{OK})$ に対する電子署名 $Sig$ とを、電子機器10に対して送信する。

【0142】データ送受信システムにおいては、ステップS191において、電子機器10は、認証装置30から暗号化警告情報 $E(PK_M, MSG_{alert})$ 及び電子署名 $Sig$ を受信すると、ステップS192において、CPU11の制御のもとに、電子署名 $Sig$ の検証

を行うことによって暗号化警告情報E (PKM, MSG alert) の検証を行う。

【0143】データ送受信システムにおいては、電子機器10による暗号化警告情報E (PKM, MSG alert) の検証の結果、暗号化警告情報E (PKM, MSG alert) が不当なものであると判定された場合には、ステップS193において、電子機器10は、警告として、暗号化警告情報エラーを示す制御信号を通信部18を介して認証装置30に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化警告情報エラーを示す制御信号を認証装置30が受信すると、認証装置30は、エラー終了する。

【0144】一方、データ送受信システムにおいては、電子機器10による暗号化警告情報E (PKM, MSG alert) の検証の結果、暗号化警告情報E (PKM, MSG alert) が正当なものであると判定された場合には、複製機器が存在していることを示すことから、ステップS193において、電子機器10は、警告を発し、認証装置30に対してその旨を通知するとともに、複製機器に対抗するための上述したような所定の処理へと移行する。

【0145】また、データ送受信システムにおいては、ステップS194において、電子機器10は、認証装置30から暗号化受諾情報E (PKM, MSG OK) 及び電子署名sigを受信すると、ステップS195において、CPU11の制御のもとに、電子署名sigの検証を行うことによって暗号化受諾情報E (PKM, MSG OK) の検証を行う。

【0146】データ送受信システムにおいては、電子機器10による暗号化受諾情報E (PKM, MSG OK) の検証の結果、暗号化受諾情報E (PKM, MSG OK) が不当なものであると判定された場合には、ステップS193において、電子機器10は、警告として、暗号化受諾情報エラーを示す制御信号を通信部18を介して認証装置30に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化受諾情報エラーを示す制御信号を認証装置30が受信すると、認証装置30は、エラー終了する。

【0147】一方、データ送受信システムにおいては、電子機器10による暗号化受諾情報E (PKM, MSG OK) の検証の結果、暗号化受諾情報E (PKM, MSG OK) が正当なものであると判定された場合には、複製機器が存在していないことを示すことから、ステップS196において、電子機器10は、鍵データの更新処理へと移行し、先に図10に示した更新処理のフローにしたがって、先に図11に示したような処理を行い、認証装置30に対する公開鍵データの更新を行う。

【0148】このように、データ送受信システムは、鍵データの更新間隔の整合性の検証を認証装置30の側で

行うことによって、複製機器を追跡してその存在を検出することができる。

【0149】最後に、鍵データの更新間隔の整合性の検証を電子機器10及び認証装置30の両者によって行う場合について、図16を用いて説明する。

【0150】データ送受信システムにおいては、同図に示すように、ステップS201において、電子機器10は、CPU11の制御のもとに、上述したタイマーが計数するタイマー値が“0”であるか否かを判定する。データ送受信システムにおいては、タイマー値が“0”でないものと判定された場合には、ステップS202において、電子機器10は、CPU11の制御のもとに、タイマー値を“1”だけデクリメントさせ、タイマー値が“0”であるか否かを再度判定する。

【0151】そして、データ送受信システムにおいては、電子機器10は、このような処理をタイマー値が“0”となるまで繰り返し、タイマー値が“0”であるものと判定された場合には、ステップS203において、CPU11の制御のもとに、乱数発生部15によって乱数値tを発生し、ステップS204において、CPU11の制御のもとに、この乱数値tが所定の範囲 $T_1 \leq t \leq T_2$ を満たすか否かを判定する。データ送受信システムにおいては、電子機器10は、乱数値tが所定の範囲 $T_1 \leq t \leq T_2$ を満たさない場合には、ステップS203からの処理を繰り返し、発生した乱数値tが所定の範囲 $T_1 \leq t \leq T_2$ を満たすまで、乱数値tを発生する。

【0152】データ送受信システムにおいては、電子機器10は、乱数値tが所定の範囲 $T_1 \leq t \leq T_2$ を満たす場合には、ステップS205において、CPU11の制御のもとに、この乱数値tを次の鍵データの更新までの時間timer\_nとしてEEPROM14等に記憶させる。

【0153】これと同時に、データ送受信システムにおいては、ステップS206において、電子機器10は、認証装置30に対して、CPU11の制御のもとに、最後に鍵データを更新した時刻を示す更新時刻情報Tlastのリクエストを行う旨の所定の制御信号と、鍵データの更新のリクエストを行う旨の所定の制御信号とを通信部18を介して送信する。なお、ここでの更新時刻情報Tlastは、上述したように、最後に先に図11に示したステップS142及びステップS143にて新たな公開鍵データPKMnewをリポジトリに記憶させて更新した時刻を示すものとする。いずれにせよ、認証装置30は、この更新時刻情報Tlastをリポジトリ等に記憶している必要がある。

【0154】以後、データ送受信システムにおいては、電子機器10による鍵データの更新間隔の整合性の検証と、認証装置30による鍵データの更新間隔の整合性の検証とを並列的に行う。

【0155】データ送受信システムにおいては、ステッ



ブS207において、認証装置30は、リクエストを受信すると、電子機器10の公開鍵データPKMを用いてリクエストされた更新時刻情報Tlastを暗号化し、暗号化更新時刻情報E(PKM, Tlast)を生成するとともに、認証機関CAの秘密鍵データSKCAを用いて暗号化更新時刻情報E(PKM, Tlast)の電子署名Sigを生成し、ステップS208において、レスポンスとして、生成した暗号化更新時刻情報E(PKM, Tlast)と、この暗号化更新時刻情報E(PKM, Tlast)に対する電子署名Sigとを、電子機器10に対して送信する。また、データ送受信システムにおいては、ステップS209において、認証装置30は、更新時刻情報Tlastと、電子機器10によってアクセスされた時刻を示すアクセス時刻情報Tacsとを用いて、

$$T_1 \leq (T_{acs} - T_{last}) + \varepsilon \leq T_2$$

を満たすか否かを判定する。ここで、定数 $\varepsilon$ は、上述したように、電子機器10と認証装置30との間でのパケットの受け渡しに要する時間や、電子機器10の内部での処理時間等を吸収する固定値である。また、アクセス時刻情報Tacsは、このステップS209における時刻を示すものとする。

【0156】データ送受信システムにおいては、 $T_1 \leq (T_{acs} - T_{last}) + \varepsilon \leq T_2$ を満たすものと判定された場合には、認証装置30は、電子機器10の公開鍵データPKMを用いて、鍵データの更新のリクエストを受諾する旨を示す検証結果情報としての受諾情報MSGOKを暗号化し、暗号化受諾情報E(PKM, MSGOK)を生成するとともに、認証機関CAの秘密鍵データSKCAを用いて暗号化受諾情報E(PKM, MSGOK)の電子署名Sigを生成し、ステップS210において、レスポンスとして、生成した暗号化受諾情報E(PKM, MSGOK)と、この暗号化受諾情報E(PKM, MSGOK)に対する電子署名Sigとを、電子機器10に対して送信する。

【0157】一方、データ送受信システムにおいては、 $T_1 \leq (T_{acs} - T_{last}) + \varepsilon \leq T_2$ を満たさないものと判定された場合には、認証装置30は、電子機器10の公開鍵データPKMを用いて、鍵データの更新のリクエストを拒否する旨を示す検証結果情報としての警告情報MSGalertを暗号化し、暗号化警告情報E(PKM, MSGalert)を生成するとともに、認証機関CAの秘密鍵データSKCAを用いて暗号化警告情報E(PKM, MSGalert)の電子署名Sigを生成し、ステップS211において、レスポンスとして、生成した暗号化警告情報E(PKM, MSGalert)と、この暗号化警告情報E(PKM, MSGalert)に対する電子署名Sigとを、電子機器10に対して送信する。

【0158】データ送受信システムにおいては、ステッ

ブS212において、電子機器10は、認証装置30から暗号化更新時刻情報E(PKM, Tlast)及び電子署名Sigを受信すると、ステップS213において、CPU11の制御のもとに、電子署名Sigの検証を行うことによって暗号化更新時刻情報E(PKM, Tlast)の検証を行う。

【0159】データ送受信システムにおいては、電子機器10による暗号化更新時刻情報E(PKM, Tlast)の検証の結果、暗号化更新時刻情報E(PKM, Tlast)が不当なものであると判定された場合には、ステップS220において、電子機器10は、警告として、暗号化更新時刻情報エラーを示す制御信号を通信部18を介して認証装置30に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化更新時刻情報エラーを示す制御信号を認証装置30が受信すると、認証装置30は、エラー終了する。

【0160】一方、データ送受信システムにおいては、電子機器10による暗号化更新時刻情報E(PKM, Tlast)の検証の結果、暗号化更新時刻情報E(PKM, Tlast)が正当なものであると判定された場合には、ステップS214において、電子機器10は、CPU11の制御のもとに、現在時刻を示す現在時刻情報Tnowと、暗号化／復号部17によって暗号化更新時刻情報E(PKM, Tlast)を復号して得られた更新時刻情報Tlastと、上述した前回のタイマー値timerとに基づいて、

$$T_{now} - (T_{last} + \text{timer}) \leq \varepsilon$$

を満たすか否かを判定する。なお、現在時刻情報Tnowは、このステップS214における時刻を示すものとする。

【0161】データ送受信システムにおいては、 $T_{now} - (T_{last} + \text{timer}) \leq \varepsilon$ を満たすものと判定された場合には、複製機器が存在していないことを示すことから、ステップS217において、電子機器10は、鍵データの更新処理へと移行し、先に図10に示した更新処理のプロトコルにしたがって、先に図11に示したような処理を行い、認証装置30に対する公開鍵データの更新を行う。

【0162】一方、データ送受信システムにおいては、 $T_{now} - (T_{last} + \text{timer}) \leq \varepsilon$ を満たさないものと判定された場合には、複製機器が存在していることを示すことから、ステップS220において、電子機器10は、警告を発し、認証装置30に対してその旨を通知するとともに、複製機器に対抗するための上述したような所定の処理へと移行する。

【0163】また、データ送受信システムにおいては、ステップS215において、電子機器10は、認証装置30から暗号化受諾情報E(PKM, MSGOK)及び電子署名Sigを受信すると、ステップS216におい



て、CPU11の制御のもとに、電子署名Sigの検証を行うことによって暗号化受諾情報E(PKM, MSGOK)の検証を行う。

【0164】データ送受信システムにおいては、電子機器10による暗号化受諾情報E(PKM, MSGOK)の検証の結果、暗号化受諾情報E(PKM, MSGOK)が不当なものであると判定された場合には、ステップS220において、電子機器10は、警告として、暗号化受諾情報エラーを示す制御信号を通信部18を介して認証装置30に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化受諾情報エラーを示す制御信号を認証装置30が受信すると、認証装置30は、エラー終了する。

【0165】一方、データ送受信システムにおいては、電子機器10による暗号化受諾情報E(PKM, MSGOK)の検証の結果、暗号化受諾情報E(PKM, MSGOK)が正当なものであると判定された場合には、複製機器が存在していないことを示すことから、ステップS217において、電子機器10は、鍵データの更新処理へと移行し、先に図10に示した更新処理のprotocolsにしたがって、先に図11に示したような処理を行い、認証装置30に対する公開鍵データの更新を行う。

【0166】さらに、データ送受信システムにおいては、ステップS218において、電子機器10は、認証装置30から暗号化警告情報E(PKM, MSGalert)及び電子署名Sigを受信すると、ステップS219において、CPU11の制御のもとに、電子署名Sigの検証を行うことによって暗号化警告情報E(PKM, MSGalert)の検証を行う。

【0167】データ送受信システムにおいては、電子機器10による暗号化警告情報E(PKM, MSGalert)の検証の結果、暗号化警告情報E(PKM, MSGalert)が不当なものであると判定された場合には、ステップS220において、電子機器10は、警告として、暗号化警告情報エラーを示す制御信号を通信部18を介して認証装置30に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化警告情報エラーを示す制御信号を認証装置30が受信すると、認証装置30は、エラー終了する。

【0168】一方、データ送受信システムにおいては、電子機器10による暗号化警告情報E(PKM, MSGalert)の検証の結果、暗号化警告情報E(PKM, MSGalert)が正当なものであると判定された場合には、複製機器が存在していることを示すことから、ステップS220において、電子機器10は、警告を発し、認証装置30に対してその旨を通知するとともに、複製機器に対抗するための上述したような所定の処理へと移行する。

【0169】このように、データ送受信システムは、鍵

データの更新間隔の整合性の検証を電子機器10及び認証装置30の両者で行うことによって、複製機器を追跡してその存在を検出することができる。

【0170】なお、ここでは、電子機器10による鍵データの更新間隔の整合性の検証結果と、認証装置30による鍵データの更新間隔の整合性の検証結果とが同一であるか否かにかかわらず、各検証結果に応じて公開鍵データの更新を行うか警告を発するかを決定しているが、データ送受信システムにおいては、より厳密には、各検証結果の組み合わせに応じて以後の処理を決定するのが望ましい。

【0171】具体的には、検証結果の組み合わせとしては、電子機器10による検証結果及び認証装置30による検証結果の両者が正当、すなわち、複製機器が存在していないことを示す結果である場合、電子機器10による検証結果は正当であるものの、認証装置30による検証結果が不当、すなわち、複製機器が存在していることを示す結果である場合、認証装置30による検証結果は正当であるものの、電子機器10による検証結果が不当である場合、及び電子機器10による検証結果及び認証装置30による検証結果の両者が不当である場合の4つのケースが想定される。

【0172】そこで、データ送受信システムにおいては、電子機器10による検証結果及び認証装置30による検証結果の両者が正当である場合には、複製機器が確実に存在していないものとして、公開鍵データの更新処理へと移行し、電子機器10による検証結果及び認証装置30による検証結果の両者が不当である場合には、複製機器が確実に存在しているものとして、複製機器に対抗するための上述したような所定の処理へと移行する。

【0173】一方、データ送受信システムにおいては、電子機器10による検証結果と認証装置30による検証結果とが異なるものである場合には、図16に示す処理を再度行うか、複製機器が存在している可能性がある旨を結果として判定するか、一方で不当であれば不当として複製機器に対抗するための上述したような所定の処理へと移行するか、又は今回は正当であるものとし、次の検証の際に今回の結果を反映させ、判断を繰り返すといった処理を行うことができる。

【0174】このように、データ送受信システムは、鍵データの更新間隔の整合性の検証を行うことにより、複製機器を追跡してその存在を検出することができる。この際、データ送受信システムにおいては、電子機器10又は複製機器と認証装置30との間で行われる通信によって得られる上述した各種情報を用いた総合的な判断を行うことにより、複製機器の存在の検出のみならず、複製機器の割り出しを行うことも可能となる。

【0175】以上説明したように、データ送受信システムは、従来の共通鍵暗号方式に基づく機器間認証を行うことなく、公開鍵暗号方式に基づく機器間認証を行うこ

とができ、鍵データの更新間隔の整合性を検証することにより、不完全な複製機器が接続された場合のみならず、完全な複製機器が接続された場合であっても、複製機器を追跡し、複製機器の存在を検出することができる。

【0176】これにより、データ送受信システムにおいては、複製機器をネットワークから排除することができることから、上述した機器間認証によって認証された電子機器は、信頼できるものとなる。このとき、データ送受信システムにおいては、信頼できる電子機器間は、信頼できるパス (trusted path) が張られている状態となる。データ送受信システムにおいては、この信頼できる電子機器に対して新たな電子機器が接続された場合には、信頼できる電子機器と新たに接続された電子機器との間で機器間認証を行う。データ送受信システムにおいては、この機器間認証によって新たに接続された電子機器が正当なものであると認証された場合には、新たに信頼できるパスが形成される。データ送受信システムにおいては、このような手順が繰り返し行われることにより、信頼できるネットワーク (trusted network) が形成される。なお、データ送受信システムにおいては、この信頼できるネットワークを信頼できないネットワーク内に形成することが可能である。

【0177】なお、本発明は、上述した実施の形態に限定されるものではない。例えば、上述した実施の形態では、電子機器 10、20 と認証装置 30 との間で行われる通信の際に、各種通信内容を暗号化するというように、通信内容を保護する機構を設けるものとして説明したが、本発明は、いわゆる IP v 6 (Internet Protocol Version 6) を完全にサポートしている環境に適用された場合には、IP v 6 の必須機能である IPsec (IP Security) を用いることによって通信内容の保護が可能となることから、上述した通信内容を保護する機構を省略することが可能となる。

【0178】また、本発明は、上述した機器固有情報を機種毎に体系的に定めるものとした場合には、上述した信頼できるネットワーク上でのサービス内容を制限することが可能となる。

【0179】さらに、上述した実施の形態では、先に図 14 乃至図 16 に示した更新時刻情報  $T_{last}$  が最後に先に図 11 に示したステップ S142 及びステップ S143 にて新たな公開鍵データ  $PK_{New}$  をリポジトリに記憶させて更新した時刻を示すものとし、先に図 14 又は図 16 に示した現在時刻情報  $T_{now}$  及び先に図 15 又は図 16 に示したアクセス時刻情報  $T_{acc}$  が判定の際の時刻を示すものとして説明したが、本発明は、各時刻情報を必ずしもこのように定義する必要はない。すなわち、電子機器 10 が鍵データの更新間隔の整合性の検証を主に行う場合の各時刻情報は、電子機器 10 が行う一連の処理のうち所定の工程での時刻を比較できる

ものであればよく、認証装置 30 が鍵データの更新間隔の整合性の検証を主に行う場合の各時刻情報は、認証装置 30 が行う一連の処理のうち所定の工程での時刻を比較できるものであればよい。したがって、本発明は、各時刻情報として、種々のバリエーションを考えることができるものである。

【0180】さらにまた、本発明は、先に図 16 に示したように、電子機器 10 と認証装置 30 とが協調して動作する場合には、各時刻情報の全てを電子機器 10 が行う一連の処理のうち所定の工程での時刻を示すものとし、鍵データの更新間隔の整合性の検証については認証装置 30 が行うといったように、各時刻情報の取得とこれらの時刻情報を用いた鍵データの更新間隔の整合性の検証とを電子機器 10 と認証装置 30 とに振り分けることもできる。この場合、本発明においては、リクエストに際して暗号化した時刻情報を併せて送信するようにすればよい。

【0181】また、上述した実施の形態では、2つの電子機器 10、20 が接続された環境であるものとし、また、電子機器 10 の複製機器が存在する場合について説明したが、本発明は、少なくとも 2 つ以上の電子機器が相互に接続された環境にも容易に適用することができ、また、任意の電子機器の複製機器が複数存在する場合についても容易に適用することができる。

【0182】このように、本発明は、その趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

#### 【0183】

【発明の効果】以上詳細に説明したように、本発明にかかる電子機器は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備える。

【0184】したがって、本発明にかかる電子機器は、現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、更新間隔検証手段によって公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することができ、複製機器をネットワークから排除することができ

る。

【0185】また、本発明にかかる認証装置は、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置であって、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、この更新間隔検証手段による検証の結果に応じた検証結果情報を電子機器に対して送信する送信手段とを備える。

【0186】したがって、本発明にかかる認証装置は、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを更新間隔検証手段によって検証し、公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することが可能となり、複製機器をネットワークから排除することが可能となる。

【0187】さらに、本発明にかかる複製機器検出システムは、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、電子機器は、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備える。

【0188】したがって、本発明にかかる複製機器検出システムは、現在時刻情報と、電子機器によって取得した更新時刻情報と、電子機器によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することができ、複製機器をネットワークから排除することができる。

【0189】さらにまた、本発明にかかる複製機器検出方法は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器で

ある複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する電子機器による公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を電子機器によって発生する乱数発生工程と、最後に公開鍵データを更新した時刻を示す更新時刻情報を電子機器によって認証装置から取得する取得工程と、現在時刻を示す現在時刻情報と、取得工程にて取得した更新時刻情報と、乱数発生工程にて前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証する更新間隔検証工程とを備える。

【0190】したがって、本発明にかかる複製機器検出方法は、現在時刻情報と、電子機器によって取得した更新時刻情報と、電子機器によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することが可能となり、複製機器をネットワークから排除することが可能となる。

【0191】また、本発明にかかる複製機器検出システムは、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置は、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、この更新間隔検証手段による検証の結果に応じた検証結果情報を電子機器に対して送信する送信手段とを備える。

【0192】したがって、本発明にかかる複製機器検出システムは、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することができ、複製機器をネットワークから排除することができる。

【0193】さらに、本発明にかかる複製機器検出方法は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である

複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証工程と、この更新間隔検証工程による検証の結果に応じた検証結果情報を認証装置から電子機器に対して送信する送信工程とを備える。

【0194】したがって、本発明にかかる複製機器検出方法は、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することが可能となり、複製機器をネットワークから排除することが可能となる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態として示すデータ送受信システムの構成を説明するブロック図である。

【図2】同データ送受信システムを構成する電子機器の構成を説明するブロック図である。

【図3】同データ送受信システムにおける通信プロトコルを説明する図であって、同電子機器から認証機関に対して公開鍵データを登録する際の同電子機器と同認証機関における認証装置との間の通信プロトコルを説明する図である。

【図4】同データ送受信システムにおいて同電子機器から同認証機関に対して公開鍵データを登録する際の一連の処理を説明するフローチャートである。

【図5】同データ送受信システムにおける通信プロトコルを説明する図であって、2つの電子機器の間で機器間認証を行う際の同電子機器と同認証装置との間の通信プロトコルを説明する図である。

【図6】同データ送受信システムにおいて2つの電子機器の間で機器間認証を行う際の第1の処理としての一連の処理を説明するフローチャートである。

【図7】同データ送受信システムにおいて2つの電子機器の間で機器間認証を行う際の第2の処理としての一連の処理を説明するフローチャートである。

【図8】同データ送受信システムにおいて2つの電子機

器の間で機器間認証を行う際の第3の処理としての一連の処理を説明するフローチャートである。

【図9】同データ送受信システムにおいて2つの電子機器の間で機器間認証を行う際の第4の処理としての一連の処理を説明するフローチャートである。

【図10】同データ送受信システムにおける通信プロトコルを説明する図であって、同電子機器から同認証機関に対して登録又は更新された公開鍵データの更新を行う際の同電子機器と同認証装置との間の通信プロトコルを説明する図である。

【図11】同データ送受信システムにおいて同電子機器から同認証機関に対して登録又は更新された公開鍵データの更新を行う際の一連の処理を説明するフローチャートである。

【図12】同データ送受信システムにおいて同電子機器から同認証機関に対して登録又は更新された公開鍵データの更新を行うにあたって行われる動作の概念を説明するフローチャートである。

【図13】同データ送受信システムにおける公開鍵データの更新間隔のタイミングを説明する図であって、

(A)は、正当な機器である同電子機器から同認証装置に対して更新のリクエストを通知するタイミングを示し、(B)は、複製機器から同認証装置に対して更新のリクエストを通知するタイミングを示し、(C)は、同認証装置に対してリクエストの通知が到達する間隔を示す図である。

【図14】同データ送受信システムにおいて複製機器を追跡し、その存在を検出する際の一連の処理を説明するフローチャートであって、鍵データの更新間隔の整合性の検証を同電子機器によって行う場合について説明する図である。

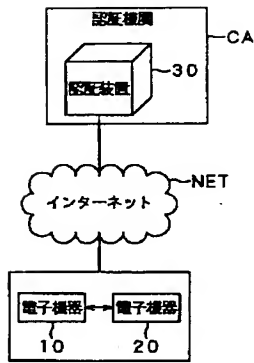
【図15】同データ送受信システムにおいて複製機器を追跡し、その存在を検出する際の一連の処理を説明するフローチャートであって、鍵データの更新間隔の整合性の検証を同認証装置によって行う場合について説明する図である。

【図16】同データ送受信システムにおいて複製機器を追跡し、その存在を検出する際の一連の処理を説明するフローチャートであって、鍵データの更新間隔の整合性の検証を同電子機器及び同認証装置の両者によって行う場合について説明する図である。

#### 【符号の説明】

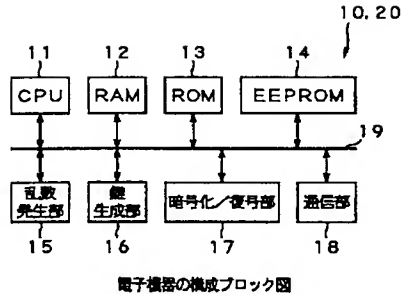
10、20 電子機器、 11 CPU、 12 RAM、 13 ROM、 14 EEPROM、 15 乱数発生部、 16 鍵生成部、 17 暗号化/復号部、 18 通信部、 30 認証装置、 CA 認証機関

【図1】



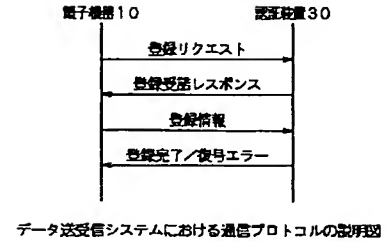
データ送受信システムの構成ブロック図

【図2】



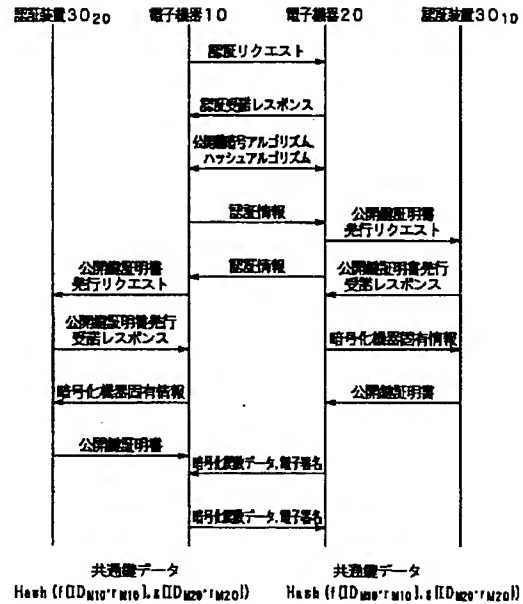
電子機器の構成ブロック図

【図3】



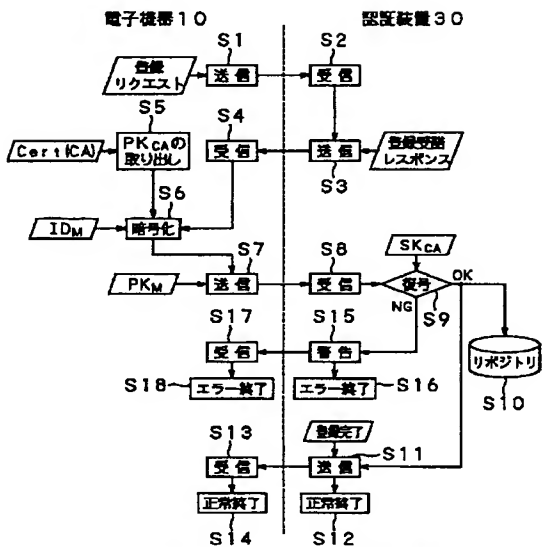
データ送受信システムにおける通信プロトコルの説明図

【図5】



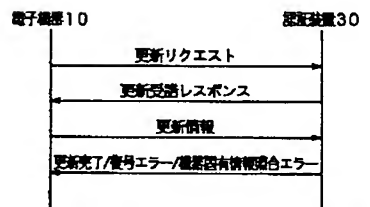
データ送受信システムにおける通信プロトコルの説明図

【図4】



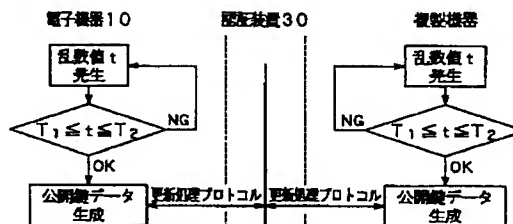
データ送受信システムにおける一連の処理工程

【図10】



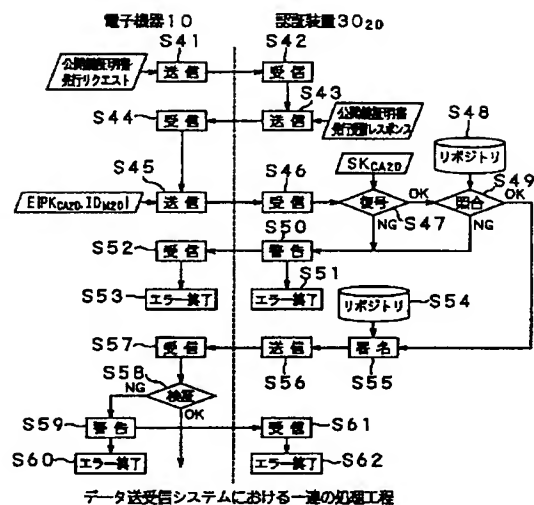
データ送受信システムにおける通信プロトコルの説明図

【図12】

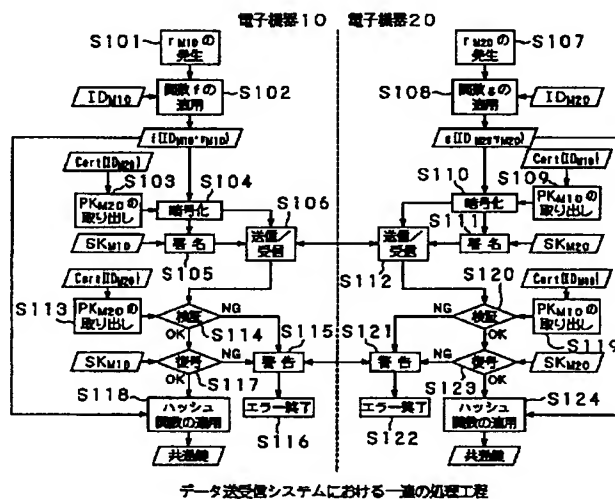


データ送受信システムにおける一連の処理工程

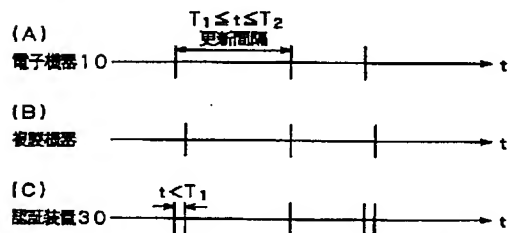
【图7】



【图9】

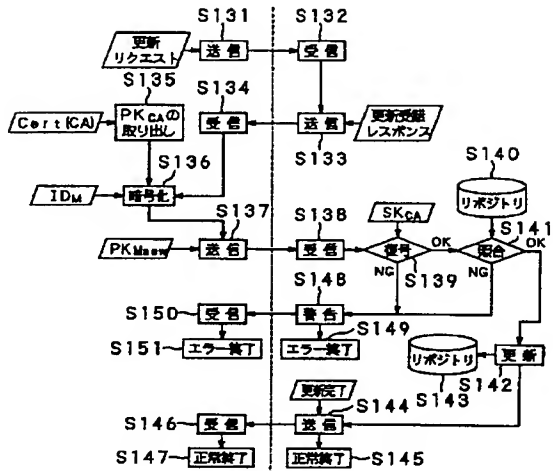


【图 13】



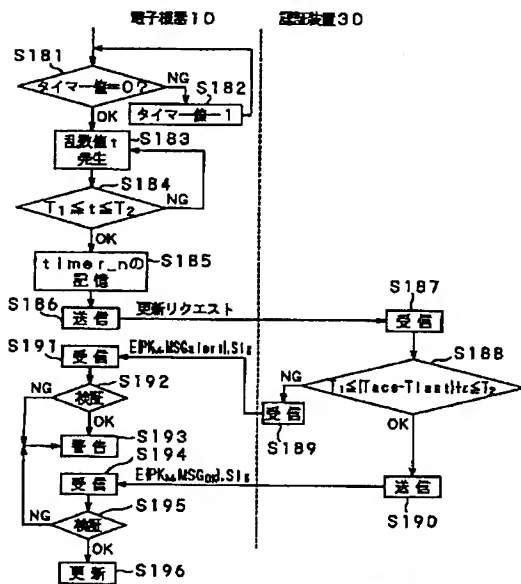
データ送受信システムにおける更新間隔のタイミングの説明図

【図11】



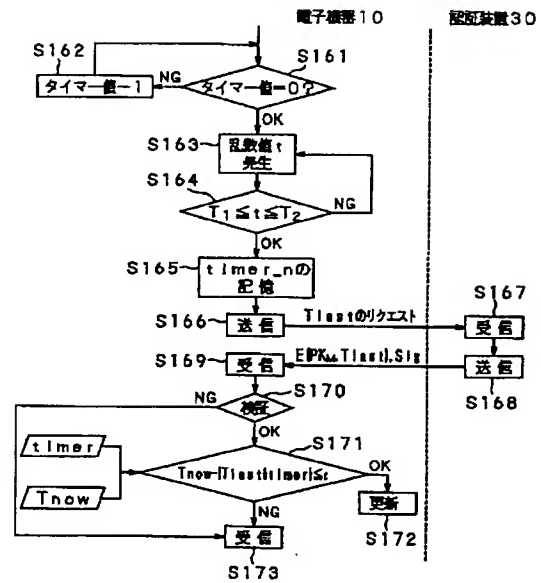
データ送受信システムにおける一連の処理工程

【図15】



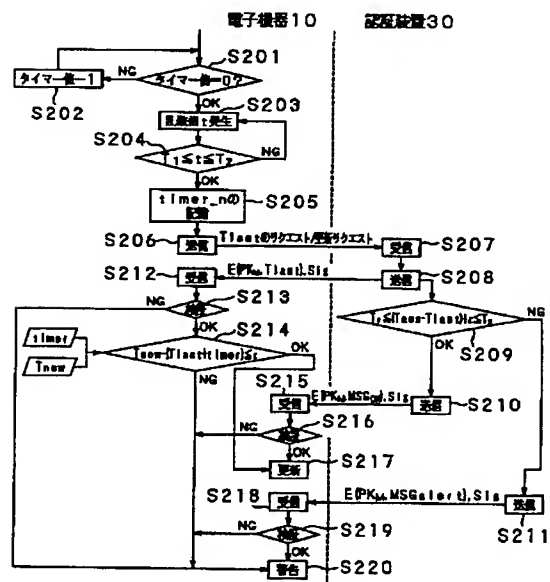
データ送受信システムにおける一連の処理工程

【図14】



データ送受信システムにおける一連の処理工程

【図16】



データ送受信システムにおける一連の処理工程



【公報種別】 特許法第 17 条の 2 の規定による補正の掲載  
【部門区分】 第 7 部門第 3 区分  
【発行日】 平成 17 年 7 月 21 日 (2005.7.21)

【公開番号】 特開 2003-163661 (P2003-163661A)  
【公開日】 平成 15 年 6 月 6 日 (2003.6.6)  
【出願番号】 特願 2001-361032 (P2001-361032)  
【国際特許分類第 7 版】

H O 4 L 9/10  
G O 9 C 1/00  
H O 4 L 9/32

【 F I 】

H O 4 L 9/00 6 2 1 A  
G O 9 C 1/00 6 4 0 E  
H O 4 L 9/00 6 7 5 D  
H O 4 L 9/00 6 7 5 B

【手続補正書】  
【提出日】 平成 16 年 11 月 29 日 (2004.11.29)  
【手続補正 1】  
【補正対象書類名】 明細書  
【補正対象項目名】 特許請求の範囲  
【補正方法】 変更  
【補正の内容】  
【特許請求の範囲】

【請求項 1】

正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器であって、

公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、

最後に公開鍵データを更新した時刻を示す更新時刻情報を上記認証装置から取得する取得手段と、

現在時刻を示す現在時刻情報と、上記取得手段によって取得した上記更新時刻情報と、上記乱数発生手段によって前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えることを特徴とする電子機器。

【請求項 2】

上記乱数発生手段によって発生した上記乱数値を、次回の公開鍵データの更新までの時間として記憶する記憶手段を備えること

を特徴とする請求項 1 記載の電子機器。

【請求項 3】

公開鍵暗号方式における復号を行う復号手段を備え、

上記取得手段は、上記認証装置によって上記更新時刻情報が暗号化された暗号化更新時刻情報を取得し、

上記復号手段は、上記暗号化更新時刻情報を復号し、上記更新時刻情報を得ることを特徴とする請求項 1 記載の電子機器。

【請求項 4】

上記暗号化更新時刻情報に対する上記認証装置の電子署名の検証を行い、上記暗号化更

新時刻情報の検証を行う更新時刻情報検証手段を備えること  
を特徴とする請求項3記載の電子機器。

【請求項5】

上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が不当なものであると判定された場合に、警告としての暗号化更新時刻情報エラーを示す制御信号を上記認証装置に対して送信する送信手段を備えること  
を特徴とする請求項4記載の電子機器。

【請求項6】

上記更新間隔検証手段は、上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が正当なものであると判定された場合に、上記公開鍵データの更新間隔の整合性の検証を行うこと  
を特徴とする請求項4記載の電子機器。

【請求項7】

公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置であって、

所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、

上記更新間隔検証手段による検証の結果に応じた検証結果情報を上記電子機器に対して送信する送信手段とを備えること  
を特徴とする認証装置。

【請求項8】

上記検証結果情報を上記正当な電子機器の公開鍵データを用いて暗号化する暗号化手段を備え、

上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報を上記電子機器に対して送信すること

を特徴とする請求項7記載の認証装置。

【請求項9】

上記認証機関の秘密鍵データを用いて上記検証結果情報の電子署名を生成する電子署名生成手段を備え、

上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報と上記電子署名とを上記電子機器に対して送信すること

を特徴とする請求項8記載の認証装置。

【請求項10】

正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、

上記電子機器は、

公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、

最後に公開鍵データを更新した時刻を示す更新時刻情報を上記認証装置から取得する取得手段と、

現在時刻を示す現在時刻情報と、上記取得手段によって取得した上記更新時刻情報と、上記乱数発生手段によって前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えること

を特徴とする複製機器検出システム。

## 【請求項 1 1】

正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、

公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する上記電子機器による公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を上記電子機器によって発生する乱数発生工程と、

最後に公開鍵データを更新した時刻を示す更新時刻情報を上記電子機器によって上記認証装置から取得する取得工程と、

現在時刻を示す現在時刻情報と、上記取得工程にて取得した上記更新時刻情報と、上記乱数発生工程にて前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記電子機器によって上記公開鍵データの更新間隔の整合性を検証する更新間隔検証工程とを備えること

を特徴とする複製機器検出方法。

## 【請求項 1 2】

正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、

公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置は、

所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、

上記更新間隔検証手段による検証の結果に応じた検証結果情報を上記電子機器に対して送信する送信手段とを備えること

を特徴とする複製機器検出システム。

## 【請求項 1 3】

正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、

所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを上記認証装置によって検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証工程と、

上記更新間隔検証工程による検証の結果に応じた検証結果情報を上記認証装置から上記電子機器に対して送信する送信工程とを備えること

を特徴とする複製機器検出方法。